# User Manual

## FaceDepot 4A

Date: December 2023

Doc Version: 1.0

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.

For further details, please visit our Company's website www.zkteco.com.

## Copyright © 2023 ZKTECO CO., LTD. All rights reserved.



## Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

## Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel has read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or

relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.zkteco.com

If there is any issue related to the product, please contact us.

## ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,
Tangxia Town, Dongguan, China.

Phone +86 769 - 82109991

Fax +86 755 - 89602394

For business related queries, please write to us at: sales@zkteco.com.

To know more about our global branches, visit www.zkteco.com.

## About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

## About the Manual

This manual introduces the operations of the **FaceDepot 4A**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Features and parameters with ★ are not available in all devices.

## Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

| For Software | |
|---|---|
| **Convention** | **Description** |
| **Bold font** | Used to identify software interface names e.g. **OK**, **Confirm**, **Cancel**. |
| > | Multi-level menus are separated by these brackets. For example, File > Create > Folder. |
| **For Device** | |
| **Convention** | **Description** |
| < > | Button or key names for devices. For example, press <OK>. |
| [ ] | Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window. |
| / | Multi-level menus are separated by forwarding slashes. For example, [File/Create/Folder]. |

Symbols

| Convention | Description |
|---|---|
|  | This implies about the notice or pays attention to, in the manual. |
|  | The general information which helps in performing the operations faster. |
|  | The information which is significant. |
|  | Care taken to avoid danger or mistakes. |
|  | The statement or event that warns of something or that serves as a cautionary example. |

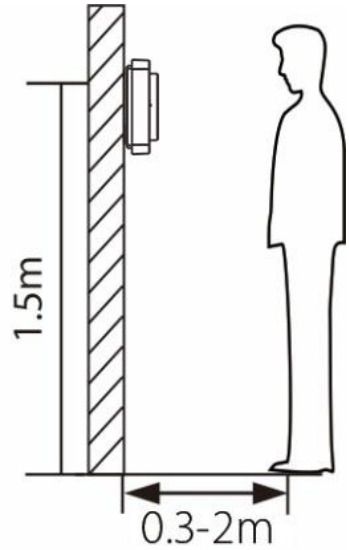
# Table of Contents

# 1 Instruction for Use

Before getting into the Device features and its functions, it is recommended to be familiar to the below fundamentals.

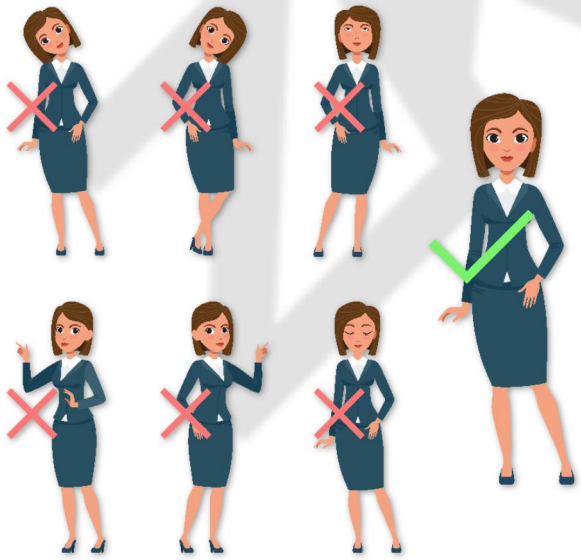
## 1.1 Standing Position, Posture and Facial Expression

- **The recommended distance**




The distance between the device and a user whose height is in a range of 1.55m to 1.85m is recommended to be 0.3 to 2m. Users may slightly move forward or backward to improve the quality of facial images captured.

- **Recommended Standing Posture and Facial Expression**



**Standing Posture**

**Facial Expression**

***Note:*** Please keep your facial expression and standing posture natural while enrolment or verification.

## 1.2 Face Template Registration

Try to keep the face in the centre of the screen during registration. Please face towards the camera and stay still during face template registration. The screen should look like this:


**Correct face registration and authentication method**

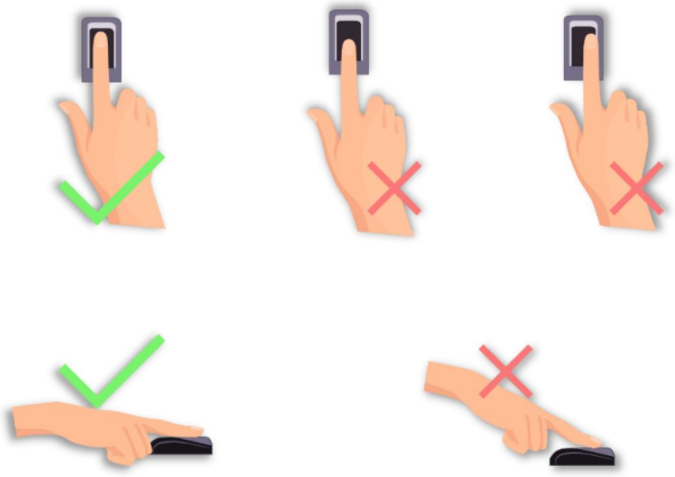
- **Recommendation for registering a face**
  - When registering a face template, maintain a distance of 40cm to 80cm between the device and the face.
  - Be careful not to change your facial expression. (Smiling face, drawn face, wink, etc.)
  - If you do not follow the instructions on the screen, the face template registration may take longer or may fail.
  - Be careful not to cover the eyes or eyebrows.
  - Do not wear hats, masks, sunglasses, or eyeglasses.
  - Be careful not to display two faces on the screen. Register one person at a time.
  - It is recommended for a user wearing glasses to register both faces with and without glasses.

- **Recommendation for authenticating a face template**
  - Ensure that the face appears inside the guideline displayed on the screen of the device.
  - If the glasses have been changed, authentication may fail. If the face without glasses has been registered, authenticate the face template without glasses further. If the face with glasses has been registered, authenticate the face with the previously worn glasses.
  - If a part of the face is covered with a hat, a mask, an eye patch, or sunglasses, authentication may fail. Do not cover the face, allow the device to recognize both the eyebrows and the face.

## 1.3 Finger Placement

Recommended fingers: Index, middle, or ring fingers.

Avoid using the thumb or pinky, as they are difficult to accurately tap onto the fingerprint reader.



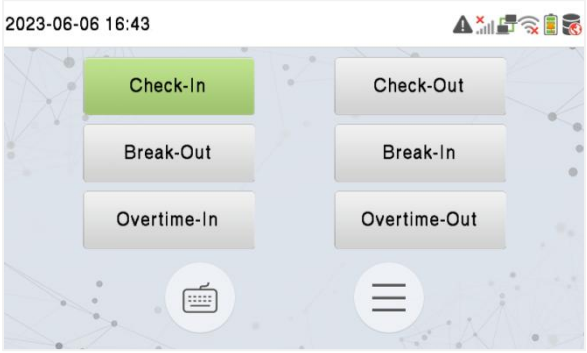
***Note:*** Please use the correct method when pressing your fingers onto the fingerprint reader for registration and identification.

## 1.4 Standby Interface

After connecting the power supply, the following standby interface is displayed:


***Note:***

1. Tap to open the interface to enter the User ID.
2. When there is no super administrator registered in the device, tap to enter the menu.
3. After setting the super administrator, it requires the super administrator's verification before entering the menu operation. For the security of the device, it is recommended to register a super administrator the first time you use the device.
4. The punch state options can also be displayed and used directly on the standby interface. Tap anywhere on the screen apart from the icons, and six shortcut keys appears on the screen, as shown in the figure below:




Press the corresponding punch state key to select your current punch state, which is displayed in green. Please refer to "Shortcut Key Mappings" for the specific operation method.

5. Note: The punch state options are off by default and need to select other mode options in the "Punch State Option" to get the punch state options on the standby screen.

## 1.5 Virtual Keyboard


***Note:*** The device supports the input of English characters, numbers, and symbols. Tap [**123**] to switch to the numeric and special character keyboard, and tap [**ABC**] to return to the alphabetic keyboard. Tap the input box, and the virtual keyboard appears. Tap [**ESC**] to exit the keyboard screen.

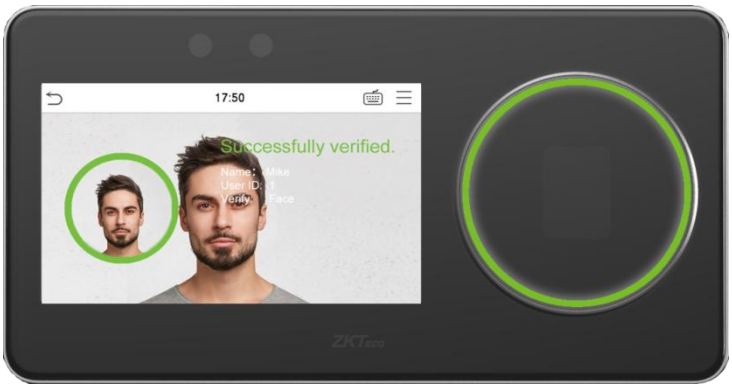
## 1.6 Verification Mode

When verification is successful, the indicator light turns green, and when verification fails, the indicator light turns red.

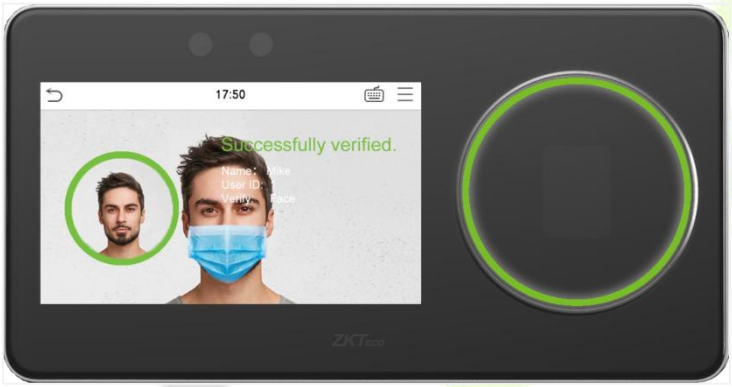
### 1.6.1 Facial Verification

**1:N Facial Verification**

In this verification mode, the device compares the collected facial images with all face data registered in the device. The following is the pop-up prompt of a successful comparison result.



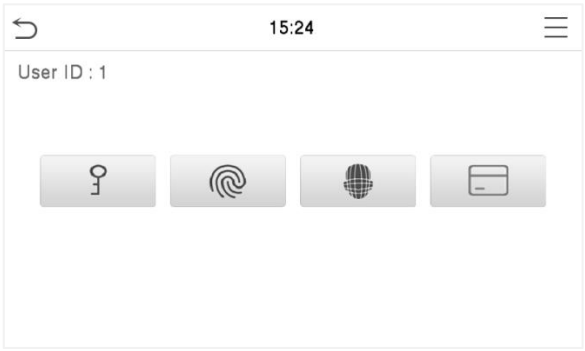

The device supports mask recognition, allowing users to be accurately recognized even if they are wearing a mask.



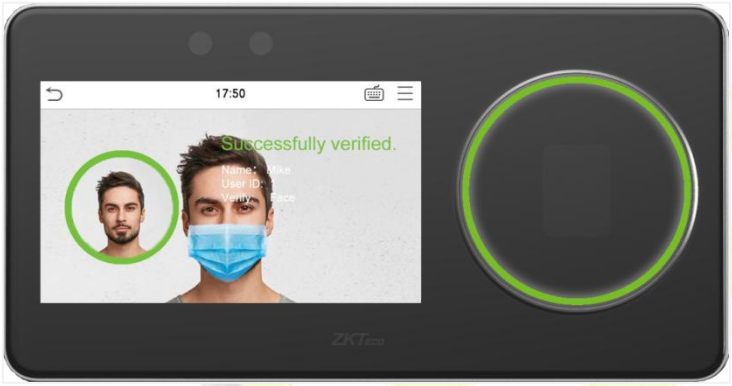

## 1:1 Facial Verification

In this verification mode, the device compares the face captured by the camera with the facial template related to the entered user ID. Tap on the main interface and enter the 1:1 facial verification mode and enter the user ID and tap [**OK**].


If the user has registered password, card and fingerprint in addition to the face, and the verification method is set to Password/Fingerprint/Card/Face, the following screen will appear. Select the icon to enter the face verification mode.




After successful verification, the prompt box displays "**Successfully verified**", as shown below:




### 1.6.2 Multi-face Template Verification

#### 1: N Multi-face Verification

In this verification mode, the device compares the obtained multi-person facial images with all the face template data stored in it. At the same time, the device can verify up to two people. The number of verification results displayed on the right side, can be customized. The image below depicts the pop-up prompt for a successful comparison result.

Tap **System** > **Face** > **Recognition Settings** > **Identifying Mode** > **Multi-face Identifying** > **Count to Display** to set the number of the verification results to be displayed.

***Note:*** The Count to Display can be set between 1 to 2.

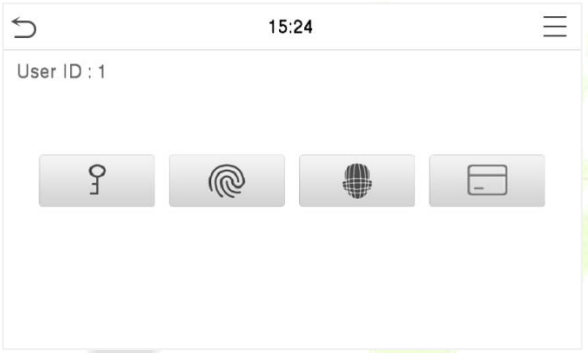


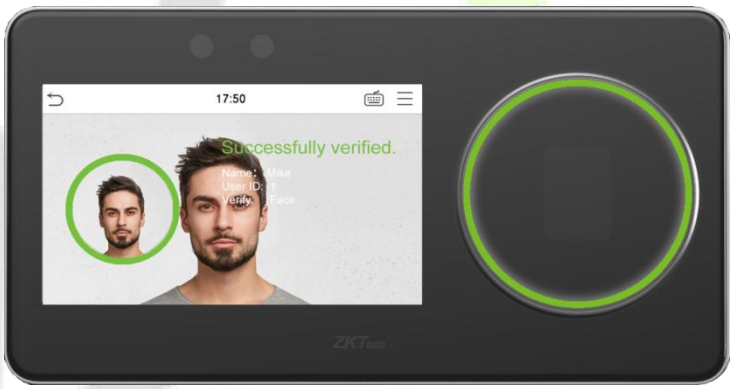
Also supports multi-person mask recognition.


## 1:1 Multi-face Verification

In this verification mode, the device compares the face captured by the camera with the facial template associated to the entered user ID. Tap on the main interface and select the 1:1 facial verification mode and enter the user ID and tap [**OK**].


If the user has registered password, card and fingerprint in addition to the face template, and the verification method is set to Password/Fingerprint/Card/Face, the following screen will appear. Select the  icon to enter the face template verification mode.




## 1.6.3 Fingerprint Verification

### 1:N Fingerprint Verification Mode

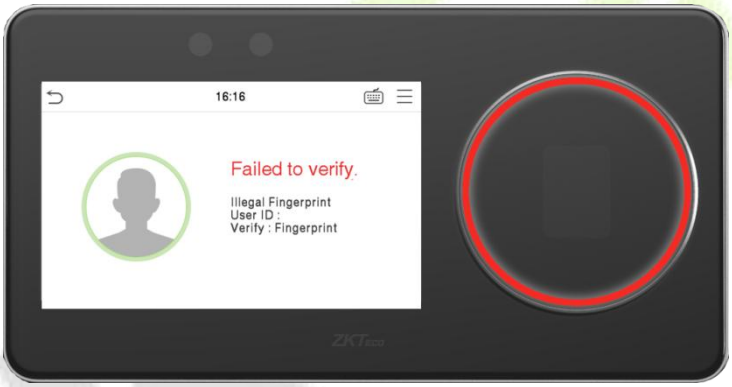
Compares the fingerprint that is being pressed onto the fingerprint reader with all of the fingerprint data that is stored in the device.

The device enters the fingerprint authentication mode when a user presses his/her finger onto the fingerprint scanner.

Please follow the correct way to place your finger onto the sensor. For details, please refer to section Finger Positioning.

**Successful Verification:**


**Failed Verification:**




## 1:1 Fingerprint Verification Mode

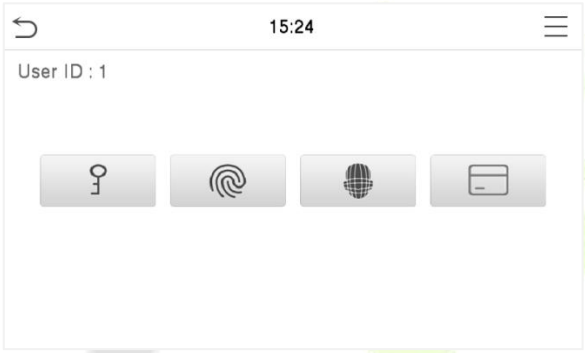
Compares the fingerprint that is being pressed onto the fingerprint reader with the fingerprints that are linked to User ID input via the virtual keyboard.

Users may verify their identities with 1:1 verification mode when they cannot gain access with 1:N authentication method.

Tap on the main interface and enter the 1:1 fingerprint verification mode.

Input the user ID and tap [**OK**].


If the user registered password, card and face in addition to the fingerprint, and the verification method is set to Password/Fingerprint/Card/Face, the following screen will appear. Select the icon to enter fingerprint verification mode.




Press the fingerprint to verify.

**Successful Verification:**

**Failed Verification:**


## 1.6.4 Card Verification ★

### 1:N Card Verification

This verification mode compares the card number in the Card induction area with all the card number data registered in the device; the following is the card verification screen.

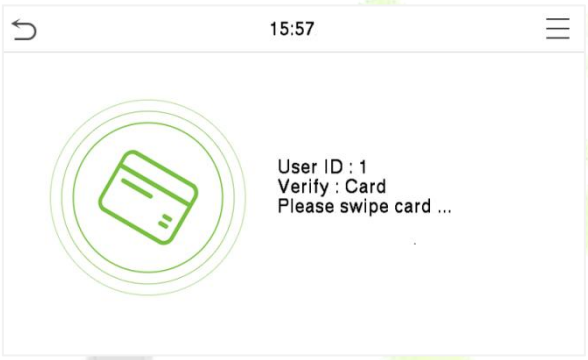

### 1:1 Card Verification

Tap the button on the main screen to open the 1:1 Card verification mode.

1. Input the user ID and tap [**OK**].

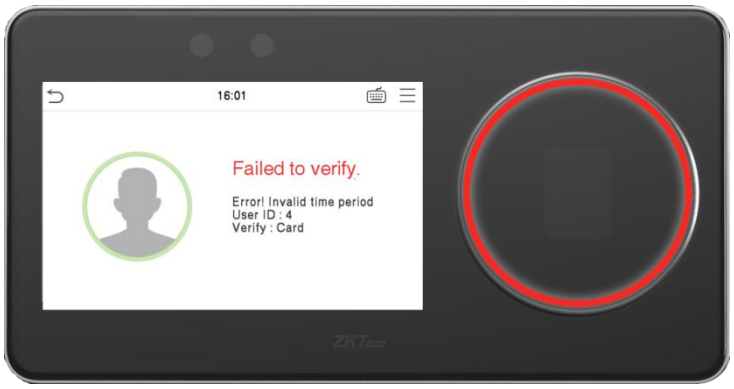
If the user has registered password, fingerprint and face in addition to card, and the verification method is set to Password/Fingerprint/Card/Face, the following screen will appear. Select the  icon to enter the card verification mode.


2. Swipe the card above the card area (the card must be registered first).




**Successful Verification:**

**Failed Verification:**




## 1.6.5 Password Verification

The Password Verification mode compares the entered password with the registered User ID and Password.

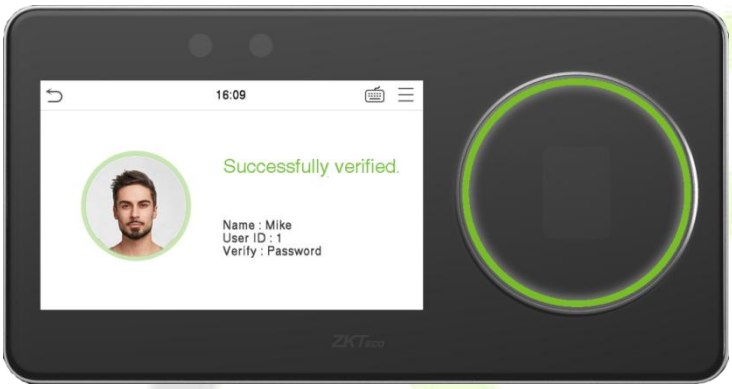
Tap the button on the main screen to open the 1:1 password verification mode.

1. Input the user ID and tap [**OK**].

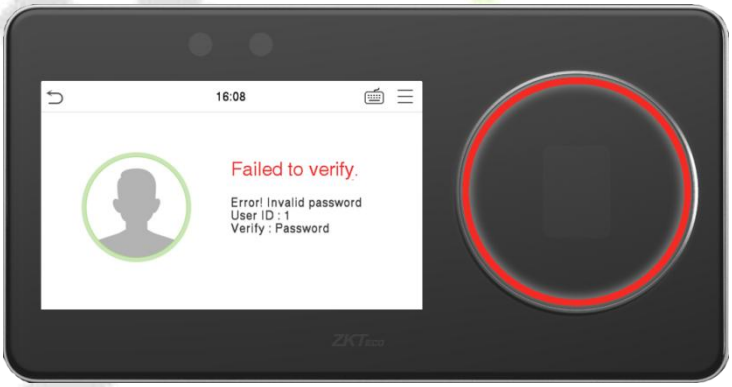

If the user registered fingerprint, card and face in addition to password, and the verification method is set to Password/Fingerprint/Card/Face, the following screen will appear. Select the icon to enter the password verification mode.

2. Input the password and tap [**OK**].


**Successful Verification:**




**Failed Verification:**

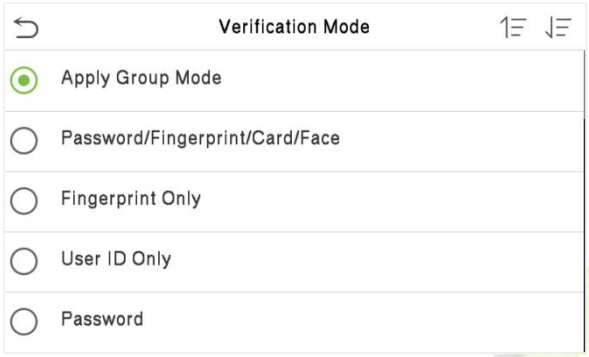


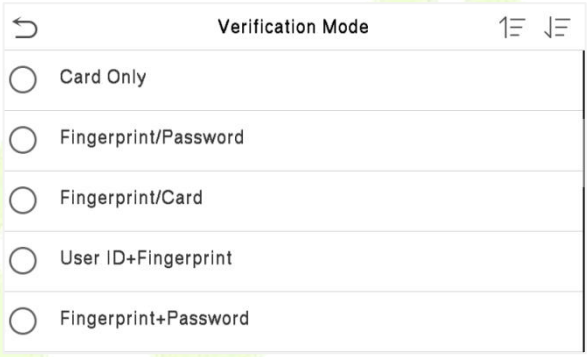

## 1.6.6 Combined Verification

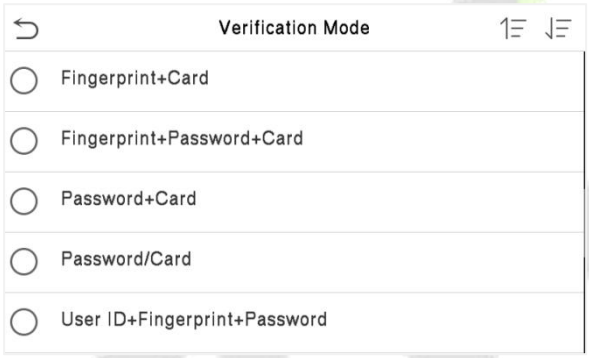
This device allows you to use a variety of verification methods to increase security. There are a total of 22 distinct verification combinations that can be implemented, as listed below:

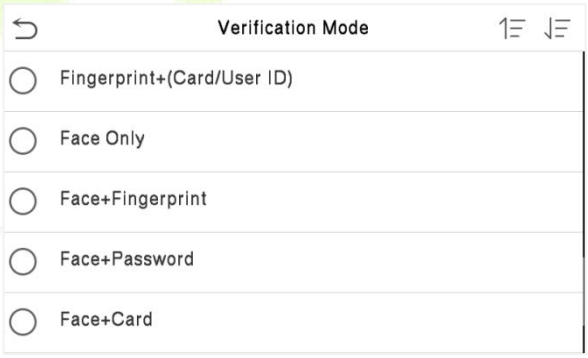
Combined Verification Symbol Definition

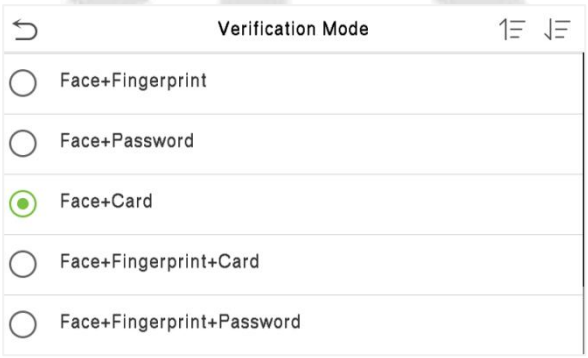
| Symbol | Definition | Explanation |
|---|---|---|
| / | or | This method compares the entered verification of a person with the related verification template previously stored to that Personnel ID in the Device. |
| + | and | This method compares the entered verification of a person with all the verification templates previously stored to that Personnel ID in the Device. |



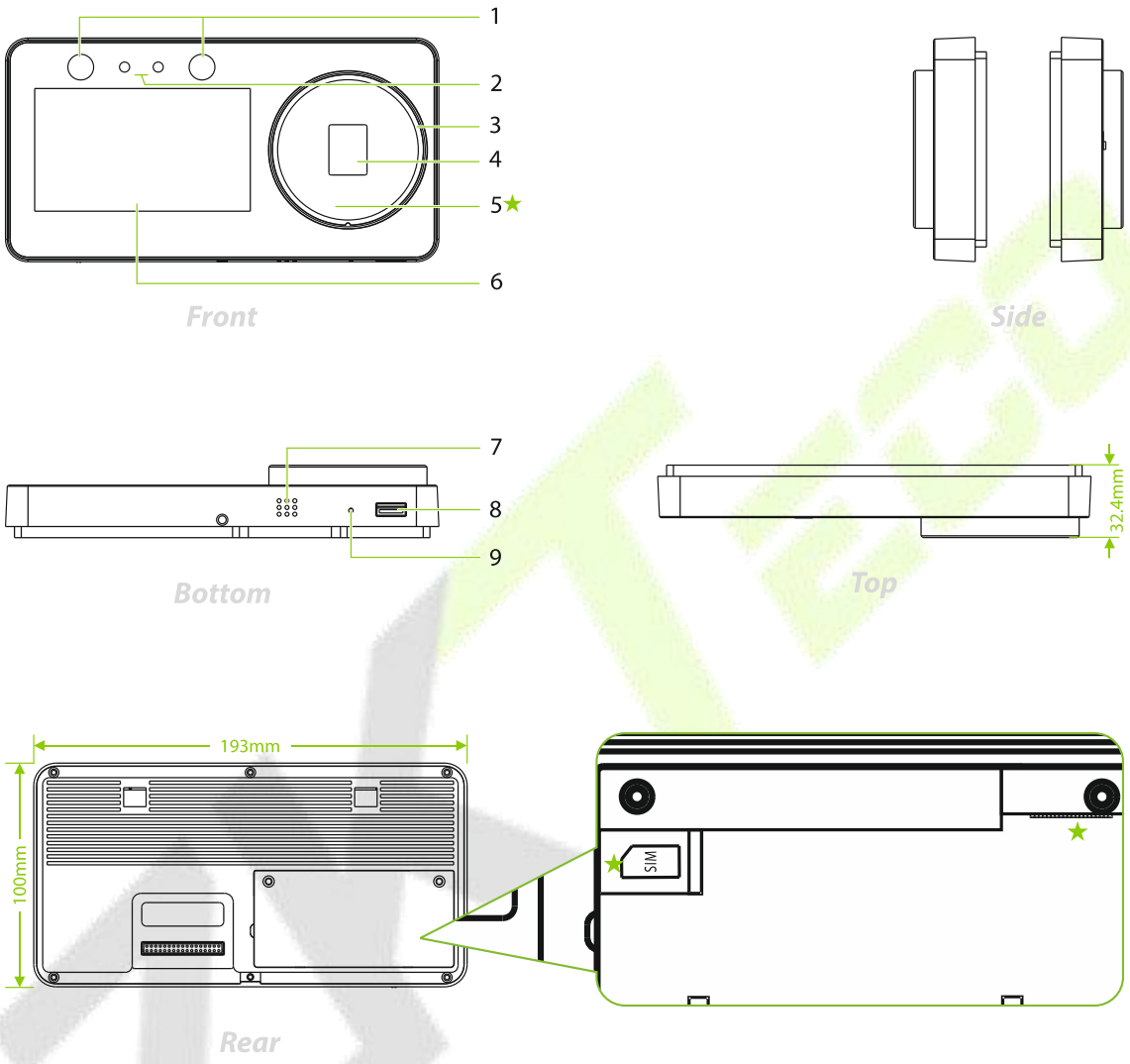

## Procedure to set for Combined Verification Mode

1. Combined verification requires personnel to register all the different verification methods. Otherwise, employees will not be able to successfully verify the combined verification process.

2. For instance, when an employee has registered only for the face data, but the Device verification mode is set as “Face + Password”, the employee will not be able to complete the verification process successfully.
3. This is because the Device compares the face template of the person with the registered verification template (both the Face and the Password) previously stored to that Personnel ID in the Device.
4. But as the employee has registered only the Face but not the Password, the verification will not get completed and the Device displays “Verification Failed”.

# 2 Overview

## 2.1 Appearance




| No. | Description |
|---|---|
| **1** | Near-Infrared Flash |
| **2** | Camera |
| **3** | Indicator Light |
| **4** | Fingerprint Sensor |
| **5** | Card Reading Area ★ |

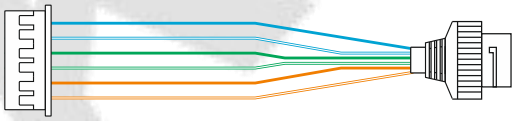
| | |
|---|---|
| **6** | 4.3-inch Touchscreen |
| **7** | Speaker |
| **8** | USB |
| **9** | Rest |

***Note:*** When verification is successful, the indicator light turns green, and when verification fails, the indicator light turns red.

## 2.2 Connection Cables and Wiring Description

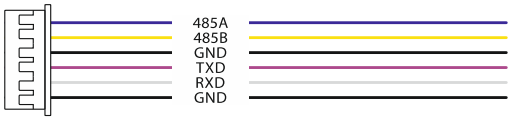
### 2.2.1 Connection Cables

| Pin | Description |
|---|---|
| **4** | Power In |

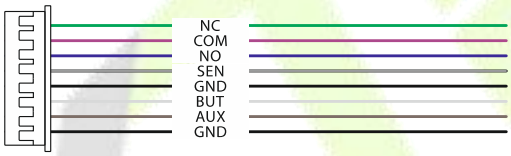


| Pin | Description |
|---|---|
| **6** | Network |

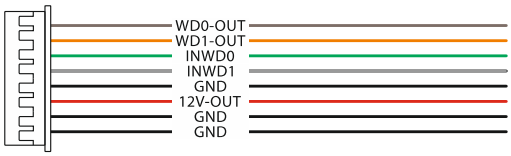

| Pin | Description | |
|---|---|---|
| **2** | ALARM+ | Alarm |
| | ALARM- | |




| Pin | Description | |
|---|---|---|
| 6 | 485A | RS485 |
| | 485B | |
| | GND | |
| | TXD | RS232 |
| | RXD | |
| | GND | |



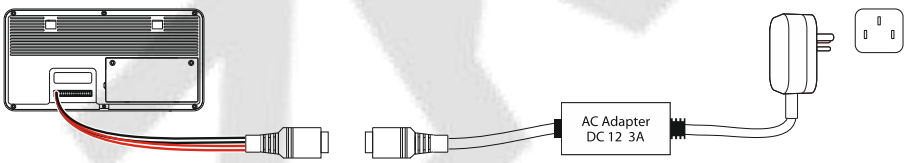

| Pin | Description | |
|---|---|---|
| 8 | NC | Lock |
| | COM | |
| | NO | |
| | SEN | Door Sensor, Exit Button |
| | GND | |
| | BUT | |
| | AUX | Auxiliary In |
| | GND | |




| Pin | Description | |
|---|---|---|
| 8 | WD0-OUT | Wiegand Out, Wiegand In |
| | WD1-OUT | |
| | INWD0 | |
| | INWD1 | |
| | GND | |
| | 12V-OUT | |
| | GND | |
| | GND | |

## 2.2.2 Wiring Description

- **Power Connection**

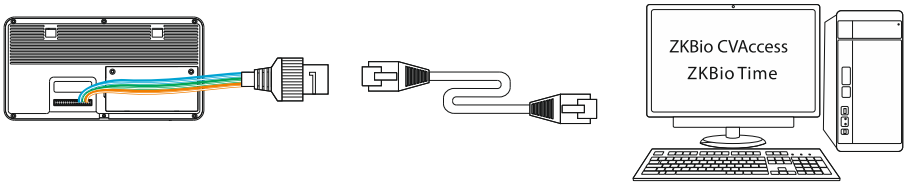



**Recommended power supply**

- Rating of 12V and 3A
- To share the power with other devices, use an AC Adapter with higher current ratings.

- **Ethernet Connection**

Connect the device and computer software over an Ethernet cable. As shown in the example below:




Default IP address: 192.168.1.201
Subnet mask: 255.255.255.0

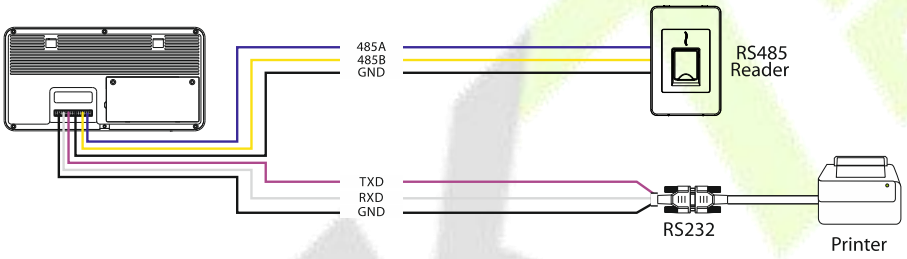
IP address: 192.168.1.130
Subnet mask: 255.255.255.0

Click on [**COMM.**] > [**Ethernet**] > [**IP Address**] , input the IP address and click on [**OK**].

***Note:*** In LAN, the IP addresses of the server (PC) and the device must be in the same network segment when connecting to the ZKBio CVAccess/ZKBio Time software.

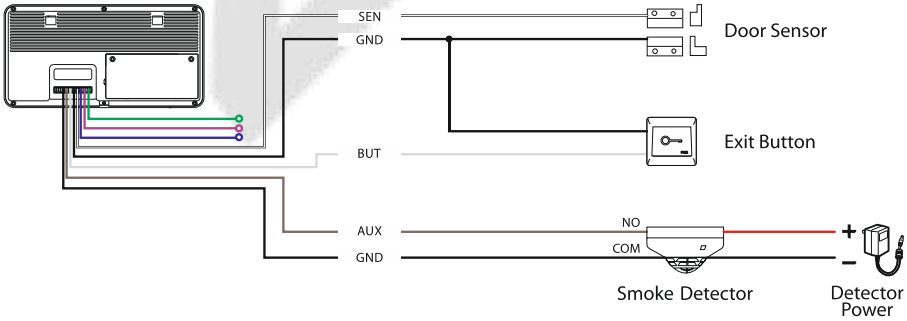
- **RS485 and RS232 Connection**

The RS485 and the RS232 lets user connect to multiple readers to the device. The RS232 and RS485 can be connected to the terminal, as shown in the figure below.



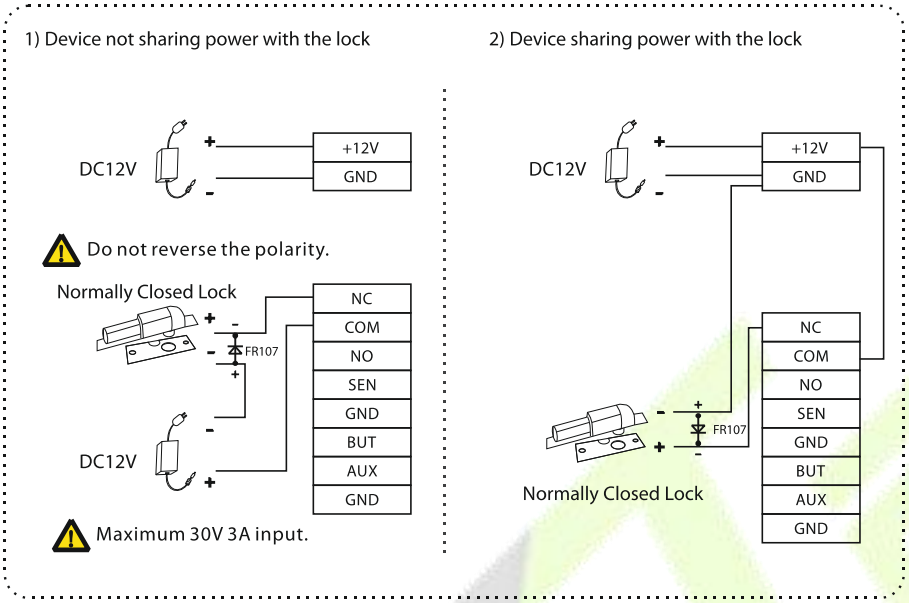

- **Alarm Connection**


- **Door Sensor, Exit Button & Auxiliary Connection**



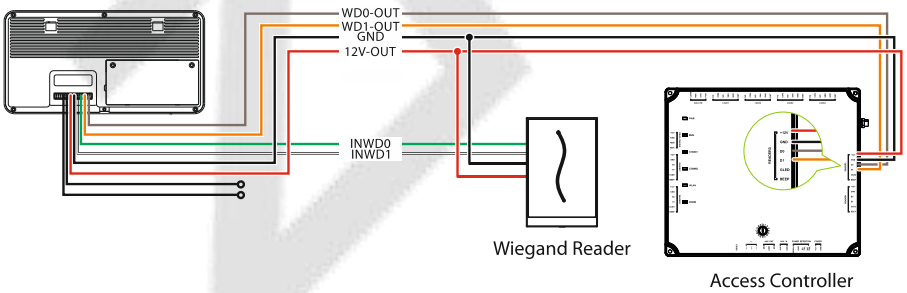
## Lock Relay Connection

The system supports both Normally Opened Lock and Normally Closed Lock. The NO Lock (normally opened when powered) is connected with 'NO1' and 'COM' terminals, and the NC Lock (normally closed when powered) is connected with 'NC1' and 'COM' terminals. The power can be shared with the lock or can be used separately for the lock, as shown in the example with NC Lock below:




## Wiegand Reader Connection

Wiegand card reader connects to the top 4 pins of the wiegand terminal and the last two pins are used by the Access controller, as shown in the following figure. It sends the credentials to the device via wiegand communication.



# 3 Installation

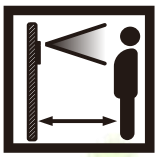
## 3.1 Installation Environment

Please refer to the following recommendations for installation.

INSTALL INDOORS ONLY

AVOID GLASS REFRACTION

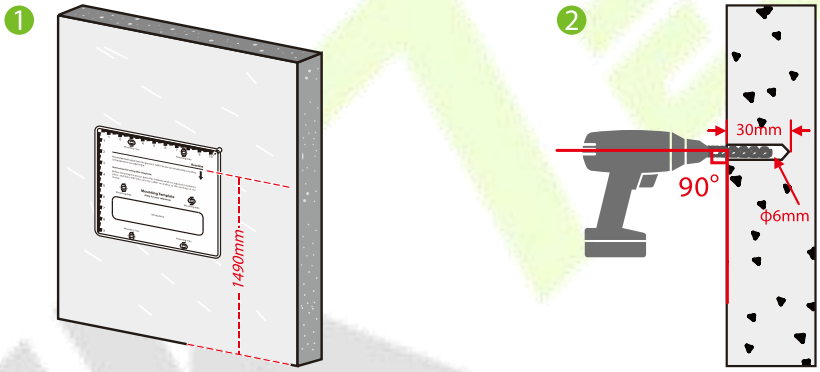
AVOID DIRECT SUNLIGHT AND EXPOSURE



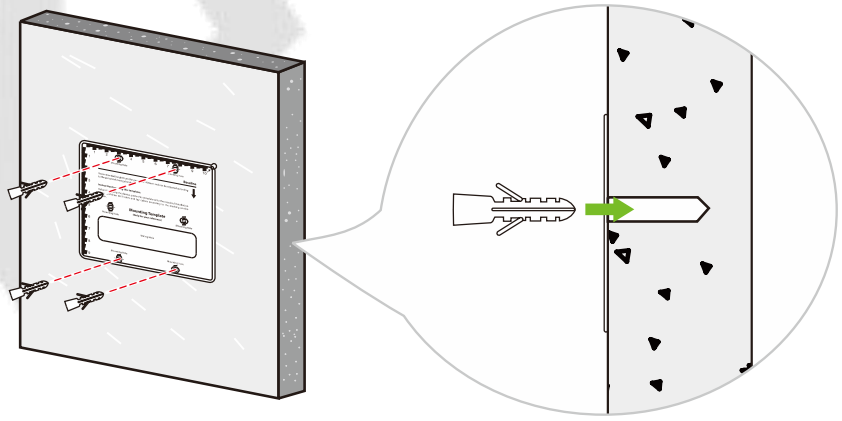
KEEP EFFECTIVE DISTANCE 0.3 to 2m

## 3.2 How to Install the Device on the Wall?

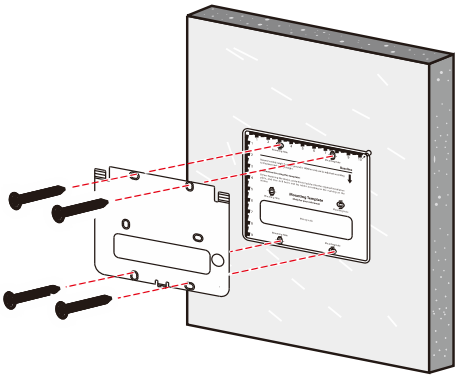
1. Stick the mounting template to the wall and drill holes according to the mounting template.



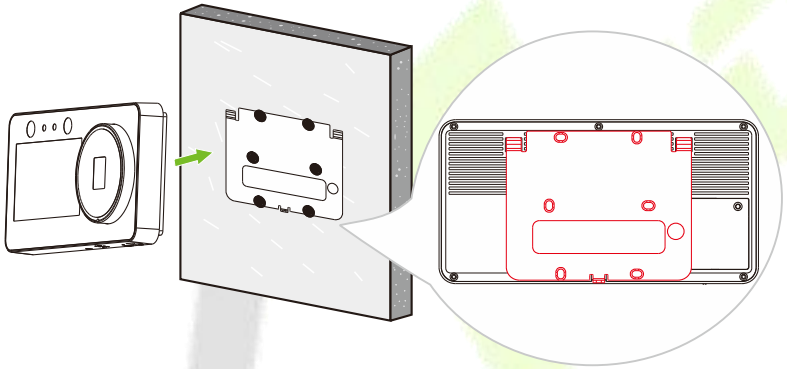

2. Insert the expansion tubes into the mounting holes.



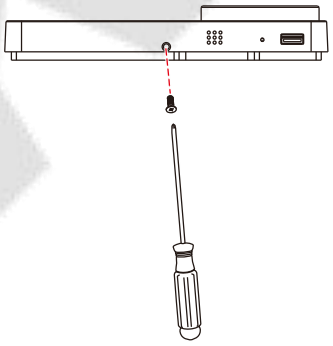
3. Attach the backplate on the wall using the wall mounting screws.



4. Attach the terminal to the backplate.

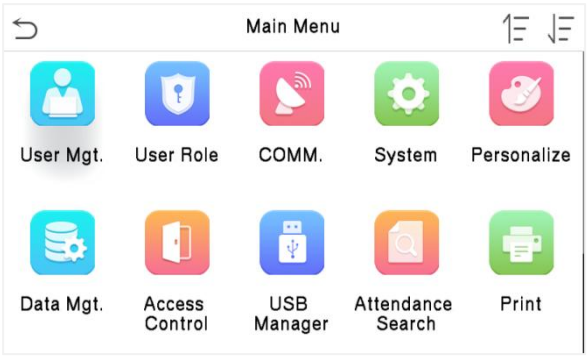


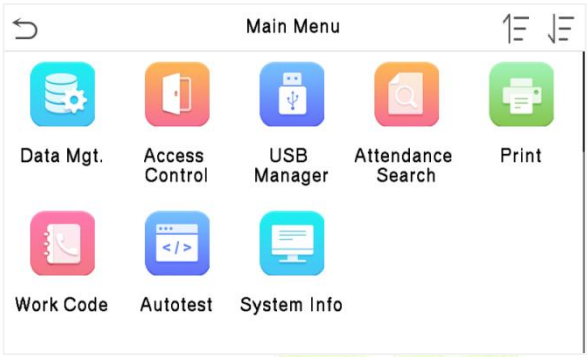
5. Fasten the terminal to the backplate with a security screw.



# 4 Main Menu

Tap  on the initial interface to enter the main menu, as shown below:

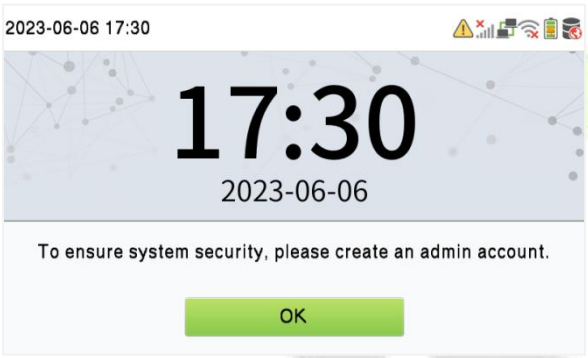


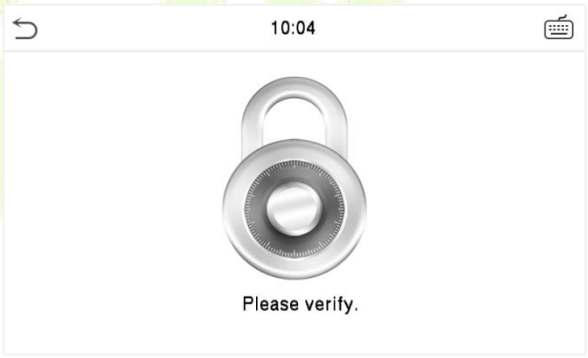




| Menu | Description |
|---|---|
| **User Mgt.** | To add, edit, view, and delete the basic information about a user. |
| **User Role** | To set the permission scope of the custom role, that is, the rights to operate the system. |
| **COMM.** | To set the relevant parameters of the network, Serial Comm, PC Connection, Cellular Data Network★, Wi-Fi★, Cloud Server, Wiegand and Network Diagnosis. |
| **System** | To set the parameters related to the system, including Date Time, Attendance, Face and Fingerprint templates, USB Upgrade, Resetting to factory settings andSecurity Settings. |
| **Personalize** | To customize settings of User Interface, Voice, Bell Schedules, Punch State Options and Shortcut Key Mappings settings. |
| **Data Mgt.** | To delete all the relevant data in the device. |
| **Access Control** | To set the parameters of the lock and the relevant access control device including options like Time Rule Setting, Holiday Settings, Access Groups, Combine Verification, Anti-passback Setup and Duress Option Settings. |
| **USB Manager** | To upload or download the specific data by a USB drive. |
| **Attendance Search** | To query the specified attendance record, check Attendance Photos and Blocklist attendance photos. |

| | |
|---|---|
| **Print** | To set printing information and functions (if the printer is connected to the device). |
| **Work Code** | Set different type of work. |
| **Autotest** | To automatically test whether each module functions properly, including the screen, audio, camera, fingerprint and real-time clock. |
| **System Info** | To view the data capacity, device and firmware information and privacy policy of the device. |

***Note:*** When users use the product for the first time, they should operate it after setting administrator privileges. Tap User Mgt. to add an administrator or edit user permissions as a super administrator. If the product does not have an administrator setting, the system will show an administrator setting command prompt every time you enter the device menu.

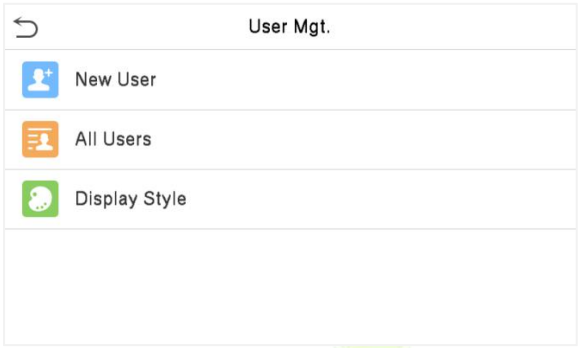


# 5 User Management

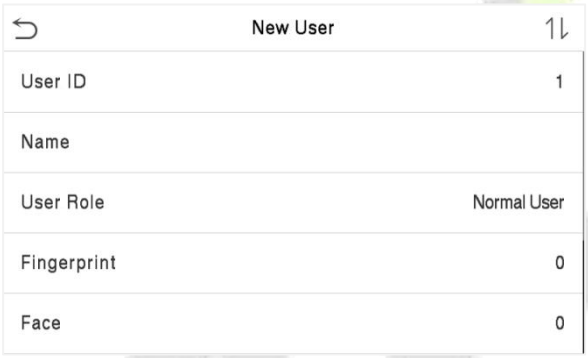
## 5.1 Add Users

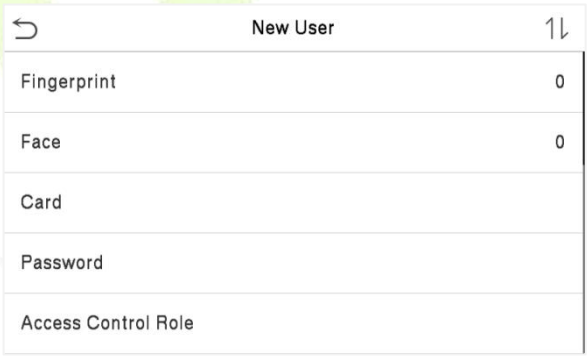
Tap **User Mgt.** on the main menu. Tap **New User**.




### 5.1.1 Register a User ID and Name

Tap **New User** and enter the **User ID** and **Name**.




***Note:***

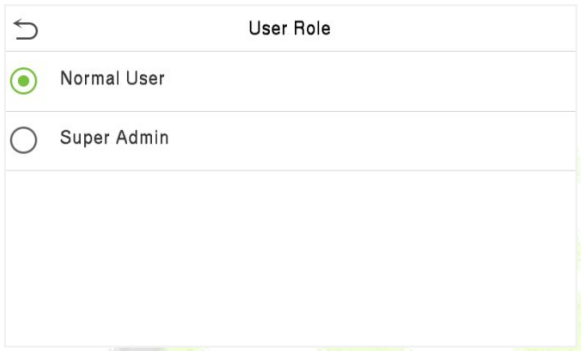
1. A username may contain 34 characters.
2. The user ID may contain 1 to 9 digits by default, support number and alphabetic.
3. During the initial registration, you can modify your ID, which cannot be modified after registration.
4. If a message "**Duplicated**" pops up, you must choose another ID.

### 5.1.2 Setting the User Role

On the **New User** interface, tap on User Role to set the user's duty as either **Normal User** or **Super Admin**.

Tap **User Role** to select **Normal User** or **Super Admin**.

- **Super Admin:** The Super Administrator owns all management privileges in the Device.
- **Normal User:** If the Super Admin is registered already in the device, then the Normal Users will not have the privilege to manage the system and can only access authentic verifications.
- **User Defined Roles:** The Normal User can also be assigned custom roles with User Defined Role. The user can be permitted to access several menu options as required.

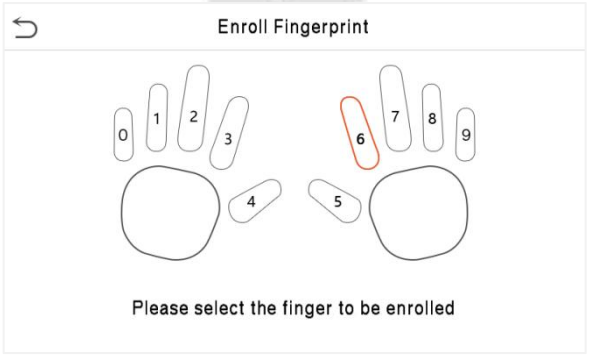



***Note:*** If the selected user role is the Super Admin, then the user must pass the identity authentication to access the main menu. The authentication is based on the authentication method(s) that the super administrator has registered.

### 5.1.3 Register Fingerprint

Tap **Fingerprint** in the **New User** interface to enter the fingerprint registration page.

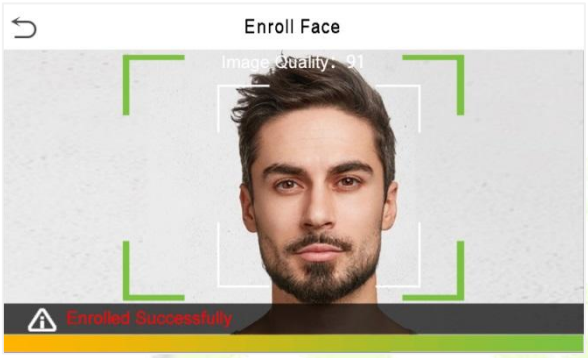
- Select the finger to be enrolled.
- Press the same finger on the fingerprint reader three times.
- Green indicates that the fingerprint was enrolled successfully.




### 5.1.4 Register Face

Tap **Face** in the **New User** interface to enter the face registration page.

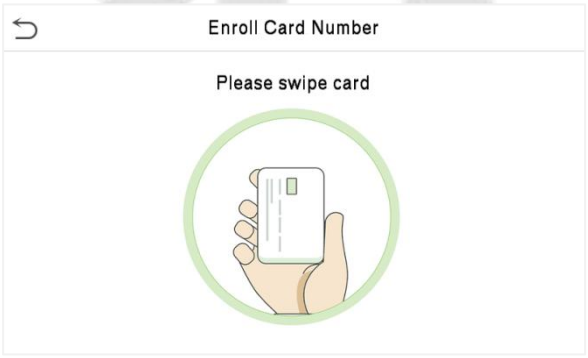
- Please face towards the camera and place yourself in such a way that your face image fits inside the white guiding box and stays still during face registration.
- A progress bar shows up while registering the face and then "**Enrolled Successfully**" message is displayed as the progress bar completes.
- If the face is registered already then, the "**Duplicated Face**" message shows up. The registration interface is as follows:

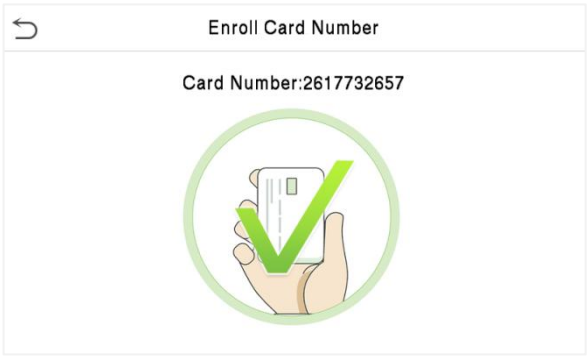



### 5.1.5 Register Card ★

Tap **Card** in the **New User** interface to enter the card registration page.

- Swipe the card underneath the card reading area on the Card interface. The registration of the card will be successful.
- If the card has already been registered, the message "**Error! Card already enrolled**" appears. The registration interface looks like this:

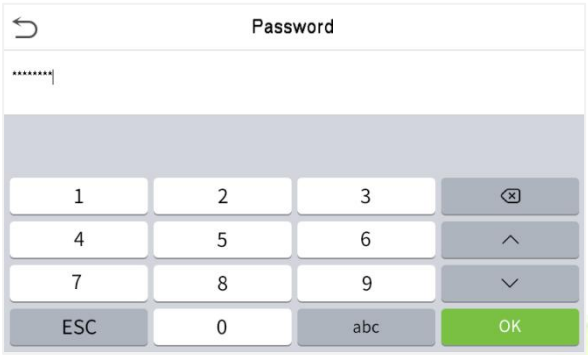


### 5.1.6 Register Password

Tap **Password** in the **New User** interface to enter the password registration page.

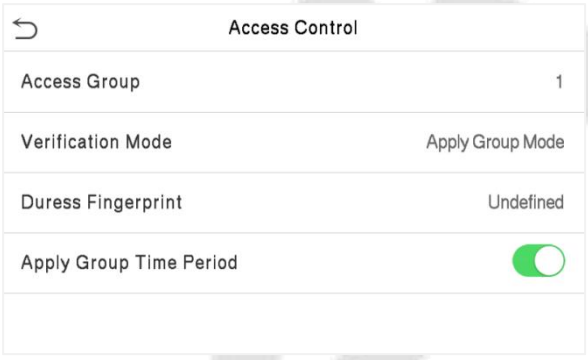
- On the Password interface, enter the required password and re-enter to confirm it and tap **OK**.
- If the re-entered password is different from the initially entered password, then the device prompts the message as "**Password not match!**", where the user needs to re-confirm the password again.
- The password may contain 1 to 8 digits by default.

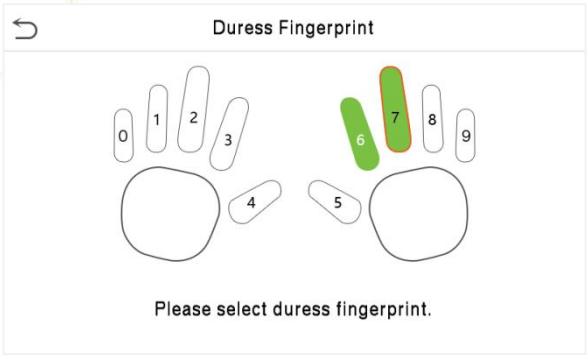




### 5.1.7 Access Control Role

The **Access Control Role** sets the door access privilege for each user. It includes the access group, verification mode and it facilitates setting the group access time period.



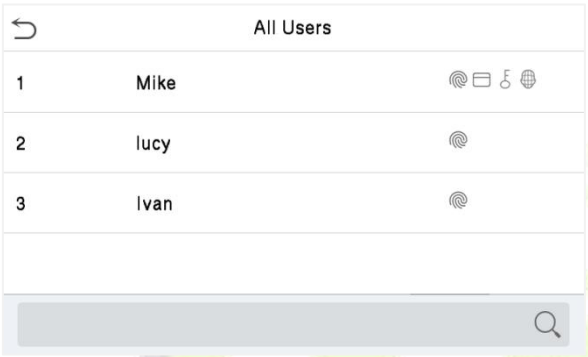

- Tap **Access Control Role** > **Access Group** to assign the registered users to different groups for better management. New users belong to Group 1 by default and can be reassigned to other groups. The device supports up to 99 Access Control groups.
- Select verification mode for the user, click **Access Control Role** > **Verification Mode**.
- The user may specify one or more fingerprints that have been registered as a duress fingerprint(s). When press the finger corresponding to the duress fingerprint on the sensor and pass the verification, the system will immediately generate a duress alarm.
- Select whether to apply the group time period for this user. It is enabled by default. If the group time period is not applied, you need to set the unlocking time for this user. The time period of this

user does not affect the time period of any other member in this group. To set the unlocking time for this user, tap **Apply Group Time Period** > Time Period 1. Enter the Time Period number and tap **OK**. 50 time periods can be set in the device and three time periods can be set for each user. For details, see Time Schedule Settings.

## 5.2 Search for Users

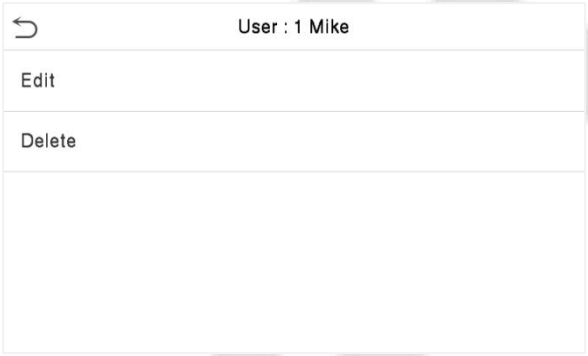
On the main menu, tap **User Mgt.**, and then tap **All Users** to search a User.

- On the **All-Users** interface, tap on the search bar on the user's list to enter the required retrieval keyword (where the keyword may be the user ID, surname, or full name) and the system will search for the related user information.




## 5.3 Edit Users

On the **All-Users** interface, tap on the required user from the list and tap **Edit** to edit the user information.

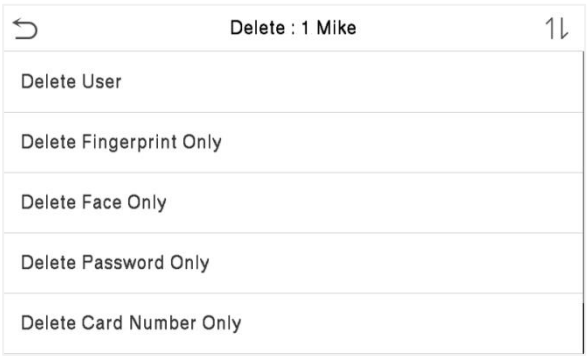


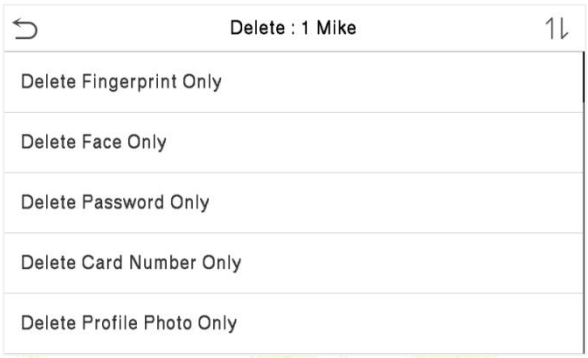


***Note:*** The operation of editing a user is the same as that of adding a user, except that the user ID cannot be modified when editing a user. For further details, refers "Add Users".

## 5.4 Delete Users

On the **All-Users** interface, tap on the required user from the list and tap **Delete** to delete the user or specific user information from the device. On the **Delete** interface, tap on the required operation, and then tap **OK** to confirm the deletion.



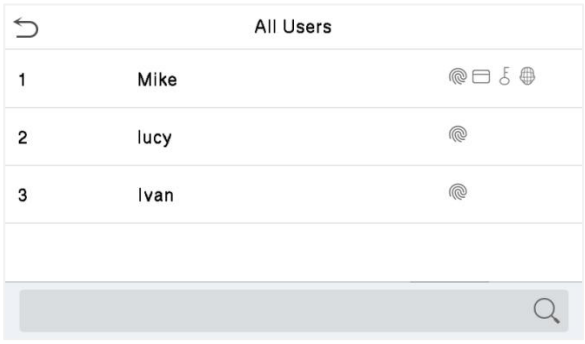

- **Delete User:** Deletes all the user information (deletes the selected User as a whole) from the Device.
- **Delete Fingerprint Only:** Deletes the fingerprint information of the selected user.
- **Delete Face Only:** Deletes the face information of the selected user.
- **Delete Password Only:** Deletes the password information of the selected user.
- **Delete Card Number Only:** Deletes the card information of the selected user.
- **Delete Profile Photo Only:** Deletes the profile photo of the selected user.

## 5.5 Display Style

On the main menu, tap **User Mgt.**, and then tap **Display Style** to enter Display Style setting interface.

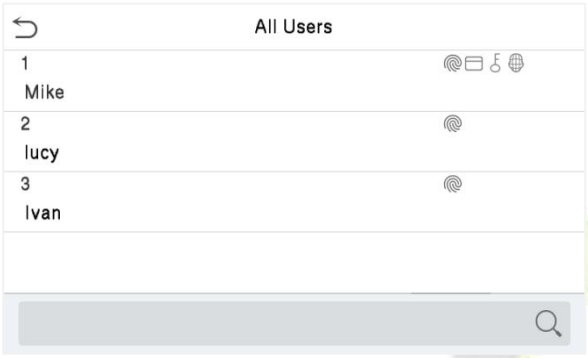

All the Display Styles are shown as below:

**Single Line:**



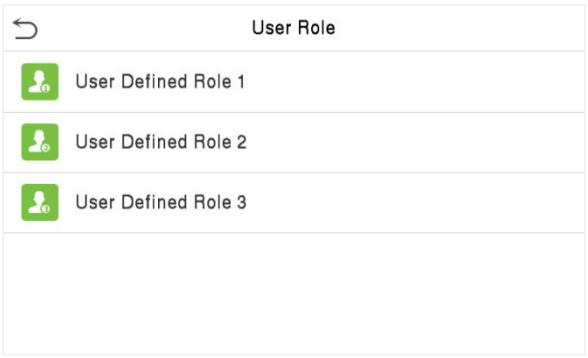

**Multiple Line:**

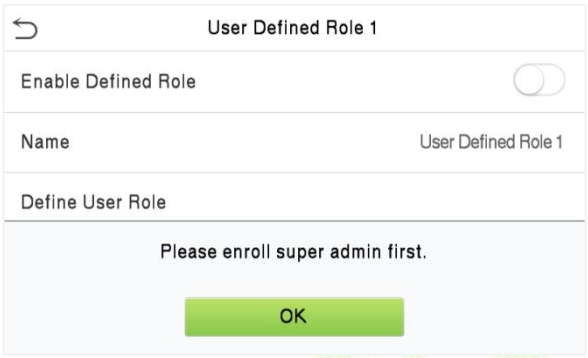

**Mixed Line:**

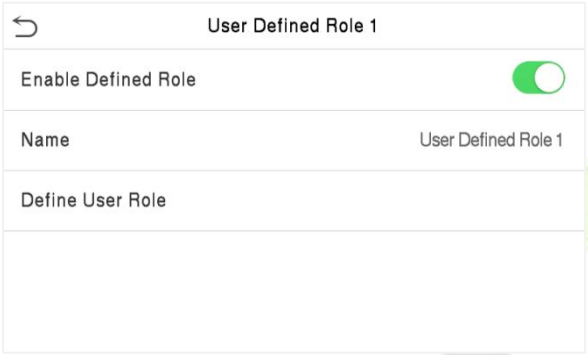


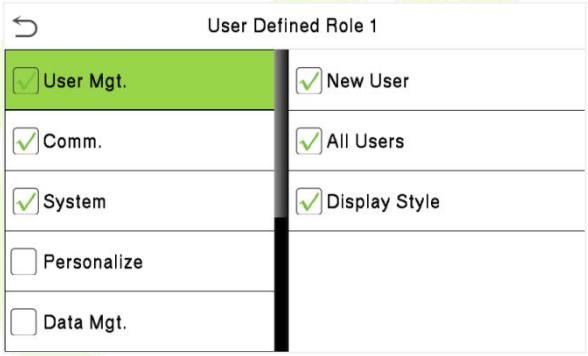
# 6 User Role

**User Role** facilitates to assign some specific permissions to certain users, based on the requirement.



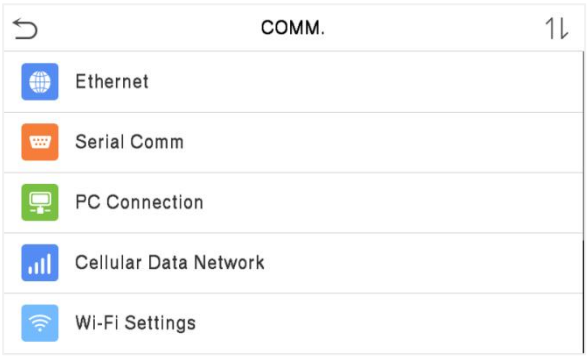

- On the main menu, tap **User Role**, and then tap on the **User Defined Role** to set the user defined permissions.
- The permission scope of the custom role can be set up into 3 roles, that is, the custom operating scope of the menu functions of the user.
- On the **User Defined Role** interface, toggle **Enable Defined Role** to enable or disable the user defined role.
- Tap on **Name** and enter the custom name of the role.
- Then, by tapping on Define User Role, select the required privileges for the new role, and then tap the Return button.
- During privilege assignment, the main menu function names will be displayed on the left and its sub-menus will be listed on the right.
- First tap on the required main menu function name, and then select its required sub-menus from the list.

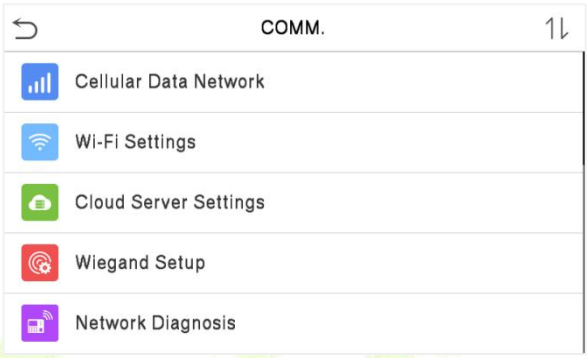
***Note:*** If the User Role is enabled for the Device, tap on **User Mgt.** > **New User** > **User Role** to assign the created roles to the required users. But if there is no super administrator registered in the Device, then the device will prompt "**Please enroll super admin first!**" when enabling the User Role function.

# 7 Communication Settings

Communication Settings are used to set the parameters of the Network, Serial Comm, PC Connection, Cellular Data Network ★, Wi-Fi ★, Cloud server, Wiegand and Network Diagnosis.

Tap **COMM.** on the main menu.

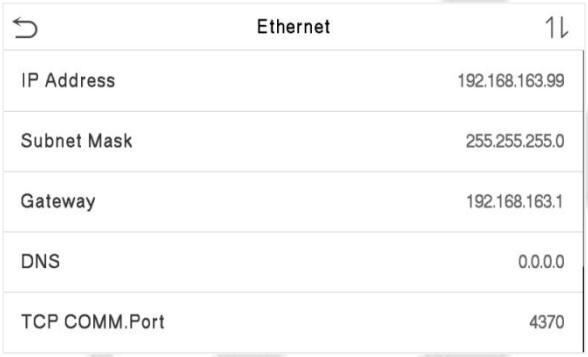


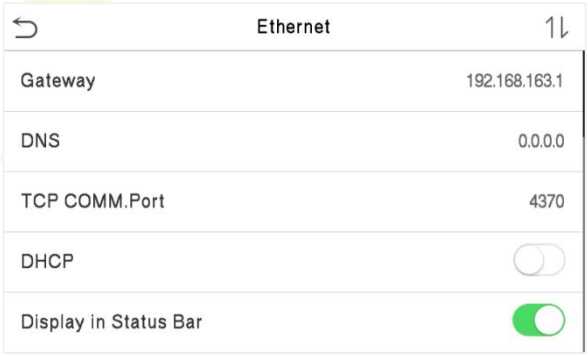




## 7.1 Network Settings

When the device needs to communicate with a PC over the Ethernet, you need to configure network settings and ensure that the device and the PC are connecting to the same network segment.

Tap **Ethernet** on the **Comm.** Settings interface.




| Menu | Description |
|---|---|
| **IP Address** | The factory default value is 192.168.1.201. Please set the IP Address as per the requirements. |
| **Subnet Mask** | The factory default value is 255.255.255.0. Please set the value as per the requirements. |
| **Gateway** | The factory default address is 0.0.0.0. Please set the value as per the requirements. |

| | |
|---|---|
| **DNS** | The factory default address is 0.0.0.0. Please set the value as per the requirements. |
| **TCP COMM. Port** | The factory default value is 4370. Please set the value as per the requirements. |
| **DHCP** | Dynamic Host Configuration Protocol, which is to dynamically allocate IP addresses for clients via server. |
| **Display in Status Bar** | To set whether to display the network icon on the status bar. |

## 7.2 Serial Comm

Serial Comm function establishes communication with the device through a serial port (RS485/Master Unit).

Tap **Serial Comm** on the **Comm.** Settings interface.

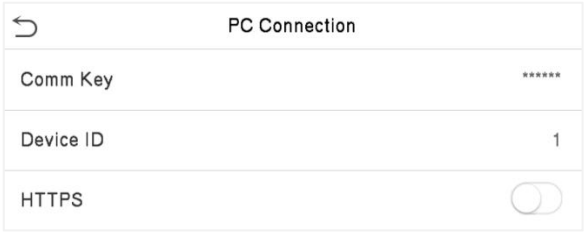


| Menu | Description |
|---|---|
| **Serial Port** | **No Using:** No communication with the device through the serial port.<br>**RS232(PC):** Communicate with the device through the RS232 serial port.<br>**Print Function:** Communicate with the print through the RS232 serial port. |
| **Baud Rate** | There are 4 baud rate options at which the data communicates with PC. They are: 115200 (default), 57600, 38400, and 19200.<br>The higher the baud rate, the faster is the communication speed, but also less reliable.<br>Hence, a higher baud rate can be used when the communication distance is short; when the communication distance is long, choosing a lower baud rate is more reliable. |

## 7.3 PC Connection

Comm Key facilitates to improve the security of the data by setting up the communication between the device and the PC. Once the Comm Key is set, a password is required to connect the device to the PC software.

Tap **PC Connection** on the **Comm.** Settings interface.




| Menu | Description |
|---|---|
| **Comm Key** | Comm Key: The default password is 0, which can be changed. The Comm Key may contain 1 to 6 digits. |
| **Device ID** | The identity number of the device, which ranges between 1 and 254.<br>If the communication method is RS232/RS485, you need to input this device ID in the software communication interface. |
| **HTTPS** | To increase the security of software access, users can enable the HTTPS protocol to create a secure and encrypted network transmission and assure the security of sent data through identity authentication and encrypted communication.<br>This function is enabled by default. This function can be enabled or disabled through the menu interface, and when changing the HTTPS status, the device will pop up a security prompt, and restart after confirmation. |

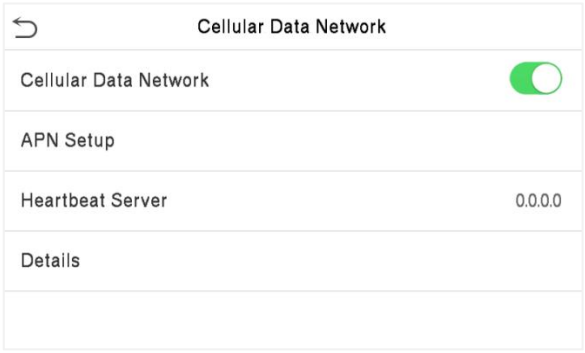
## 7.4 Cellular Data Network ★

When the equipment is in the Dial-Up Network, make sure the device is in the coverage of GPRS or WCDMA signal, and it is must know of the used modem type, APN name and access number and so on. Before enabling, please insert the All-in-one card into the 4G module first.

Tap **Cellular Data Network** on the **Comm.** Settings interface.

Toggle the button to enable the Cellular Data Network. Under normal circumstances, the device will automatically connect to the mobile network after being enabled. If you cannot connect, you can

manually set the relevant parameters to connect. When the mobile network is connected successfully, the initial interface will display the mobile network logo.




| Menu | Description |
|---|---|
| **Cellular Data Network** | Whether to enable the mobile network. |
| **APN Setup** | To set APN information, such as the dial number, user name and password.<br>**APN:** Access Point Name, provided by the operator and not supported in the CDMA network.<br>**Dial Number:** Number of the cellular data network.<br>**User Name and Password:** To verify whether the user has the privilege to use this network. |
| **Heartbeat Server** | To detect the connection status of the mobile network. The terminal periodically sends ICMP packets to the heartbeat server to detect whether the terminal is online. When the terminal is offline, the device automatically performs dial-up connection again. Therefore, when setting the heartbeat server, ensure that the heartbeat server can be pinged and remain online stably for a long term.<br>Note: Generally, the customer can set the heartbeat server address as the ADMS server address. |
| **Details** | To view the information about mobile network connection, such as network mode, IP address, received data, and sent data. |

***Note:*** When using cellular data network function, the device must be powered by external power supply; when the device is powered only by the back-up battery, the cellular data network function is automatically turned off; with external power, the user is required to manually turn on the cellular data network function switch.

## 7.5 Wi-Fi Settings ★

The device provides a Wi-Fi module, which can be built-in within the device module or can be externally connected.

The Wi-Fi module enables data transmission via Wi-Fi (Wireless Fidelity) and establishes a wireless network environment. Wi-Fi is enabled by default in the device. If you don't need to use the Wi-Fi network, you can toggle the Wi-Fi to disable the button.

Tap **Wi-Fi Settings** on the **Comm.** Settings interface to configure the Wi-Fi settings.


### Searching the Wi-Fi Network

- WIFI is enabled in the device by default. Toggle the button to enable or disable WIFI.
- Once the Wi-Fi is turned on, the device will search for the available Wi-Fi within the network range.
- Tap on the required Wi-Fi name from the available list and input the correct password in the password interface, and then tap **Connect to Wi-Fi (OK)**.
- When the WIFI is connected successfully, the initial interface will display the Wi-Fi logo.

### Adding Wi-Fi Network Manually

The Wi-Fi can also be added manually if the required Wi-Fi does not show on the list.

On this interface, enter the Wi-Fi network parameters. (The added network must exist.)

***Note:*** After successfully adding the Wi-Fi manually, follow the same process to search for the added Wi-Fi name.

### Advanced Setting

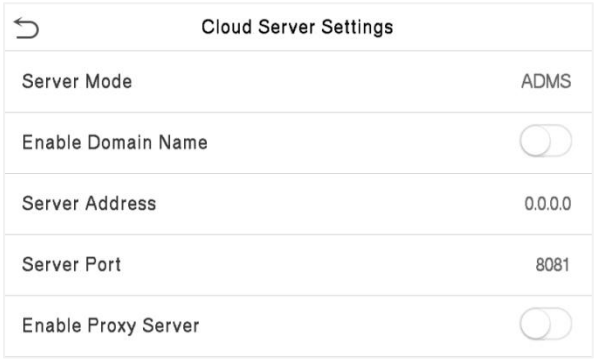
On the **Wi-Fi Settings** interface, tap on **Advanced** to set the relevant parameters as required.


| Menu | Description |
|---|---|
| **DHCP** | Dynamic Host Configuration Protocol (DHCP) dynamically allocates IP addresses to network clients. If the DHCP is enabled, then the IP cannot be set manually. |
| **IP Address** | The IP address for the Wi-Fi network, the default is 0.0.0.0. It can be modified according to the network availability. |
| **Subnet Mask** | The default Subnet Mask of the Wi-Fi network is 255.255.255.0. It can be modified according to the network availability. |
| **Gateway** | The Default Gateway address is 0.0.0.0. It can be modified according to the network availability. |
| **DNS** | The factory default address is 0.0.0.0. Please set the value as per the requirements. |

## 7.6 Cloud Server Settings

This represents the settings used for connecting the ADMS server.

Tap **Cloud Server Settings** on the **Comm.** Settings interface.



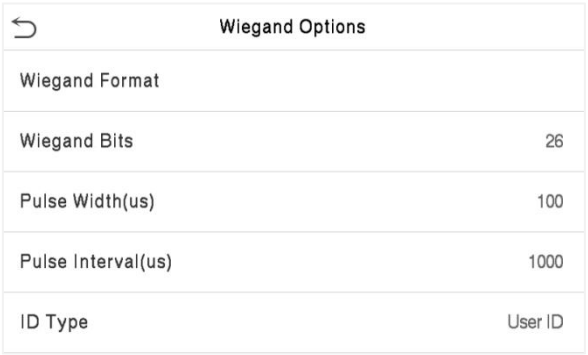

| Menu | | Description |
|---|---|---|
| **Enable Domain Name** | **Server Address** | When this function is enabled, the domain name mode "http://... "will be used, such as http://www.XYZ.com, while "XYZ" denotes the domain name when this mode is turned ON. |
| **Disable Domain Name** | **Server Address** | IP address of the ADMS server. |
| | **Server Port** | Port used by the ADMS server. |
| **Enable Proxy Server** | | When you choose to enable the proxy, you need to set the IP address and port number of the proxy server. |

## 7.7 Wiegand Setup

The menu is used to set the Wiegand Input & Output parameters.

Tap **Wiegand Setup** on the **Comm.** Settings interface.

## Wiegand Input



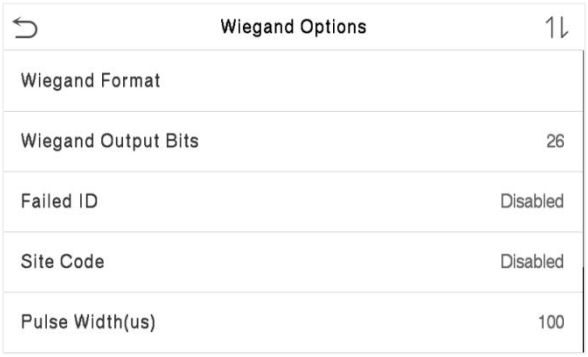

| Menu | Description |
|---|---|
| **Wiegand Format** | Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits. |
| **Wiegand Bits** | Number of bits of Wiegand data. |
| **Pulse Width(us)** | The value of the pulse width sent by Wiegand is 100 microseconds by default, which can be adjusted within the range of 20 to 400 microseconds. |
| **Pulse Interval(us)** | The default value is 1000 microseconds, which can be adjusted within the range of 200 to 20000 microseconds. |
| **ID Type** | Select between the User ID and Card number. |

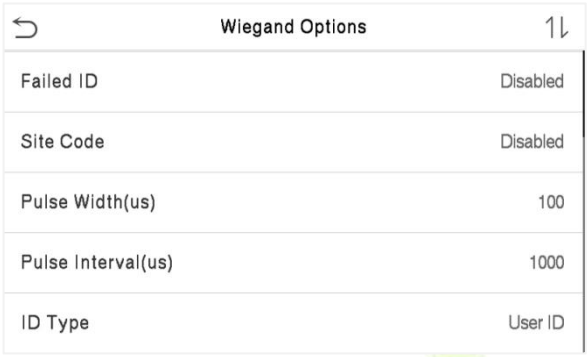
Definitions of various common Wiegand formats:

| Menu | Description |
|---|---|
| **Wiegand26** | ECCCCCCCCCCCCCCCCCCCCCCCO<br>It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 25th bits is the card numbers. |
| **Wiegand26a** | ESSSSSSSSCCCCCCCCCCCCCCCO<br>It consists of 26 bits of binary code. The 1st bit is the even parity bit of the 2nd to 13th bits, while the 26th bit is the odd parity bit of the 14th to 25th bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers. |
| **Wiegand34** | ECCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO<br>It consists of 34 bits of binary code. The 1st bit is the even parity bit of the |

| | |
|---|---|
| | 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 25th bits is the card numbers. |
| **Wiegand34a** | ESSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCO<br>It consists of 34 bits of binary code. The 1st bit is the even parity bit of the 2nd to 17th bits, while the 34th bit is the odd parity bit of the 18th to 33rd bits. The 2nd to 9th bits is the site codes, while the 10th to 25th bits are the card numbers. |
| **Wiegand36** | OFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCMME<br>It consists of 36 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 36th bit is the even parity bit of the 19th to 35th bits. The 2nd to 17th bits is the device codes. The 18th to 33rd bits is the card numbers, and the 34th to 35th bits are the manufacturer codes. |
| **Wiegand36a** | EFFFFFFFFFFFFFFFFFCCCCCCCCCCCCCCCCO<br>It consists of 36 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 36th bit is the odd parity bit of the 19th to 35th bits. The 2nd to 19th bits is the device codes, and the 20th to 35th bits are the card numbers. |
| **Wiegand37** | OMMMMSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCE<br>It consists of 37 bits of binary code. The 1st bit is the odd parity bit of the 2nd to 18th bits, while the 37th bit is the even parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 16th bits is the site codes, and the 21st to 36th bits are the card numbers. |
| **Wiegand37a** | EMMMFFFFFFFFFSSSSSSCCCCCCCCCCCCCCCCO<br>It consists of 37 bits of binary code. The 1st bit is the even parity bit of the 2nd to 18th bits, while the 37th bit is the odd parity bit of the 19th to 36th bits. The 2nd to 4th bits is the manufacturer codes. The 5th to 14th bits is the device codes, and15th to 20th bits are the site codes, and the 21st to 36th bits are the card numbers. |
| **Wiegand50** | ESSSSSSSSSSSSSSSCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCO<br>It consists of 50 bits of binary code. The 1st bit is the even parity bit of the 2nd to 25th bits, while the 50th bit is the odd parity bit of the 26th to 49th bits. The 2nd to 17th bits is the site codes, and the 18th to 49th bits are the card numbers. |
| "**C**" denotes the card number; "**E**" denotes the even parity bit; "**O**" denotes the odd parity bit;<br>"**F**" denotes the facility code; "**M**" denotes the manufacturer code; "**P**" denotes the parity bit; and "**S**" denotes the site code. | |

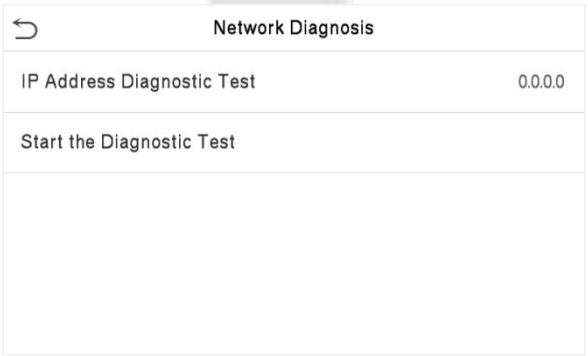
### Wiegand Output

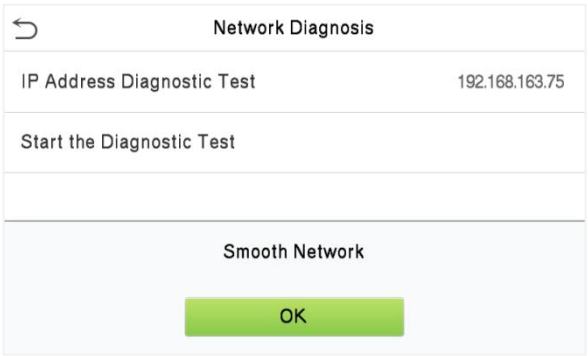



| Menu | Description |
|---|---|
| **Wiegand Format** | Values range from 26 bits, 34 bits, 36 bits, 37 bits, and 50 bits. |
| **Wiegand Output Bits** | After choosing the Wiegand format, you can select one of the corresponding output digits in the Wiegand format |
| **Failed ID** | If the verification is failed, the system will send the failed ID to the device and replace the card number or personnel ID with the new ones. |
| **Site Code** | It is similar to the Device ID. The difference is that a site code can be set manually, and is repeatable in a different device. The valid value ranges from 0 to 256 by default. |
| **Pulse Width(us)** | The pulse width represents the changes in the quantity of electric charge with high-frequency capacitance regularly within a specified time. |
| **Pulse Interval(us)** | The time interval between pulses. |
| **ID Type** | Select between the User ID and Card number. |

## 7.8 Network Diagnosis



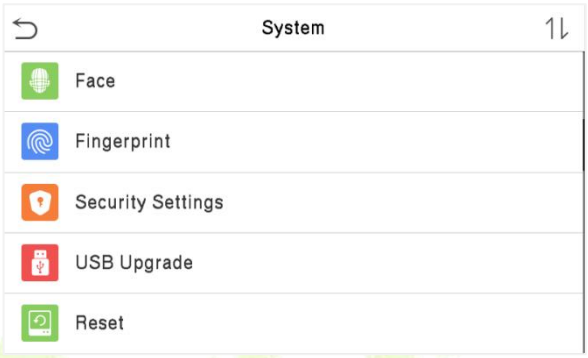



| Menu | Description |
| --- | --- |
| **IP Address Diagnostic Test** | The factory default address is 0.0.0.0. Please set the value as per the requirements. |
| **Start the Diagnostic Test** | Tap start to automatically diagnose the network. |

# 8 System Settings

The System Settings is used to set the related system parameters to optimize the performance of the device.

Tap **System** on the main menu interface.


## 8.1 Date and Time

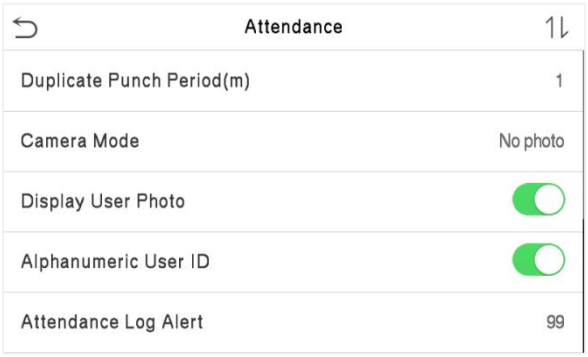
Tap **Date Time** on the **System** interface.

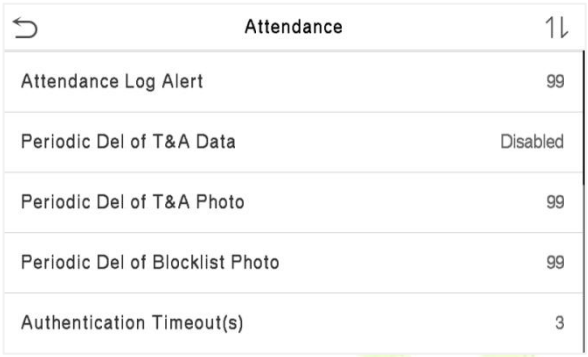

- Tap **Date and Time Auto Sync** to enable automatic time synchronization based on the service address you enter.
- Tap **Manual Date and Time** to manually set the date and time and then tap to **Confirm** and save.
- Tap **Select Time Zone** to manually select the time zone where the device is located.
- Enable or disable this format by tapping 24-Hour Time. If enabled, then select the **Date Format** to set the date.
- When restoring the factory settings, the time (24-hour) and date format (YYYY-MM-DD) can be restored, but the device date and time cannot be restored.

***Note:*** For example, the user sets the time of the device (18:35 on March 15, 2020) to 18:30 on January 1, 2021. After restoring the factory settings, the time of the device will change to 18:30, January 1, 2021.

## 8.2 Attendance

Tap **Attendance** on the **System** interface.



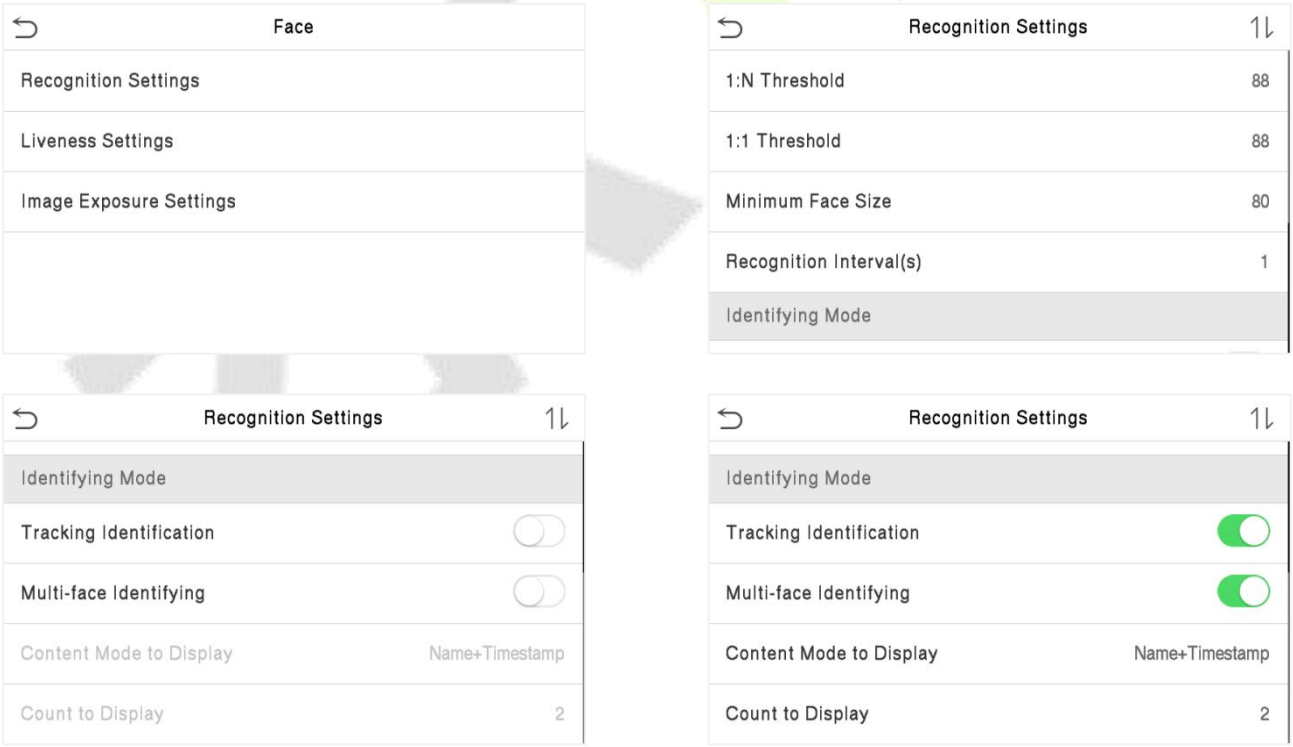



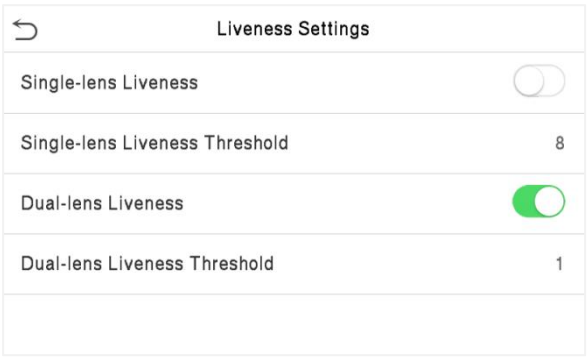

| Menu | Description |
|---|---|
| **Duplicate Punch Period (m)** | Within the set time range, the attendance record of the same person will not be saved; the valid value ranges from 1 to 999999 minutes. |
| **Camera Mode** | This function is disabled by default. When enabled, a security prompt will pop-up and the sound of shutter in the camera will turn on mandatorily. There are 5 modes:<br>**No photo:** No photo is taken during user verification.<br>**Take photo, no save:** Photo is taken but not saved during verification.<br>**Take photo and save:** All the photos taken during verification is saved.<br>**Save on successful verification:** Photo is taken and saved for each successful verification.<br>Save on failed verification: Photo is taken and saved only for each failed verification. |
| **Display User Photo** | Whether to display the user photo when the user passes the verification. |
| **Alphanumeric User ID** | Enable/Disable the alphanumeric as User ID. |
| **Attendance Log Alert** | When the record space of the attendance reaches the maximum threshold value, the device automatically displays the memory space warning.<br>Users may disable the function or set a valid value between 1 and 9999. |
| **Periodic Del of T&A Data** | When attendance logs reach its maximum capacity, the device |

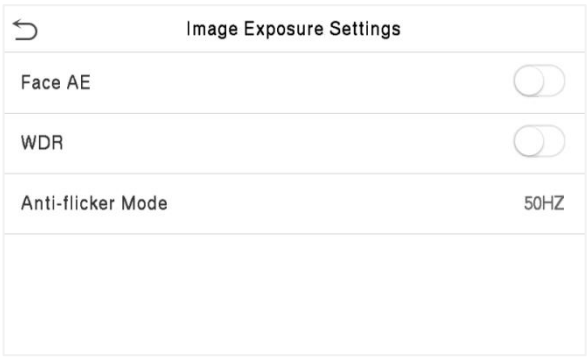
| | |
|---|---|
| | automatically deletes a set of old access logs.<br>Users may disable the function or set a valid value between 1 and 999. |
| **Periodic Del of T&A Photo** | When attendance photos reach its maximum capacity, the device automatically deletes a set of old attendance photos.<br>Users may disable the function or set a valid value between 1 and 99. |
| **Periodic Del of Blocklist Photo** | When block listed photos reach its maximum capacity, the device automatically deletes a set of old block listed photos.<br>Users may disable the function or set a valid value between 1 and 99. |
| **Authentication Timeout(s)** | The amount of time taken to display a successful verification message.<br>Valid value: 1 to 9 seconds. |

## 8.3 Face Parameters

Tap **Face** on the **System** interface.






| Menu | Description | |
|---|---|---|
| **Recognition Settings** | **1:N Threshold:** The verification will be successful only if the similarity between the acquired facial image and all registered facial templates is greater than the set value in the 1:N verification mode.<br>The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and higher is the rejection rate, and vice versa. It is recommended to set the default value of 88. | |
| | **1:1 Threshold:** Under 1:1 verification mode, the verification will only be successful when the similarity between the acquired facial image and the user's facial templates enrolled in the device is greater than the set value.<br>The valid value ranges from 0 to 100. The higher the thresholds, the lower the misjudgement rate and the higher is the rejection rate, and vice versa. It is recommended to set the default value of 88. | |
| | **Minimum Face Size:** It sets the minimum face size required for facial registration and comparison.<br>If the minimum size of the captured image is smaller than the set value, then it will be filtered off and not recognized as a face.<br>This value can also be interpreted as the face comparison distance. The farther the individual is, the smaller the face, and the smaller number of pixels of the face obtained by the algorithm. Therefore, adjusting this parameter can adjust the farthest comparison of distance of faces. When the value is 0, the face comparison distance is not limited. | |
| | **Recognition Interval(s):** After the interval identifying is clicked (selected), for example, if the comparison interval is set to 5 seconds, then the face recognition will verify the face every 5 seconds. Valid value: 0 to 9 seconds. 0 means continuous identifying, 1 to 9 means identifying at intervals. | |
| | **Identifying** | **Tracking Identification:** The same face can only be recognized once. To recognize it again, you must leave the |

| | | |
|---|---|---|
| | **Mode** | face recognition area and re-enter it before it can be recognized again. |
| | | **Multi-face Identifying:** When it is toggled on, the device can identify multiple faces at once. The Content Mode to Display, and Count to Display can be configured only if it is toggled on. |
| | | **Content Mode to Display:** You can select the content displayed below the user photo in the interface after the face verification is successful. Such as display the Name, User ID + Name, Timestamp, User ID + Timestamp, Name + Timestamp, User ID. |
| | | **Count to Display:** You can choose the number of face verification results to be displayed in the interface at once, e.g., if set to 2, the interface displays up to 2 successful user verifications at once.<br>**Note:** The Count to Display can be set from 1 to 2 users. |
| **Liveness Settings** | **Single-lens Liveness:** It detects the spoof attempt using visible light images to determine if the provided biometric source sample is of a real person (a live human being) or a false representation.<br>**Single-lens Liveness Threshold:** It facilitates judging whether the captured visible image is a real person (a live human being). The larger the value, the better the anti-spoofing performance using visible light.<br>**Dual-lens Liveness:** It uses near-infrared spectra imaging to identify and prevent fake photos and videos attack.<br>**Dual-lens Liveness Threshold:** It is convenient to judge whether the near-infrared spectral imaging is fake photo and video. The larger the value, the better the anti-spoofing performance of near-infrared spectral imaging.<br>**Note:** For the Anti-Spoofing settings, the user needs to enable both Single-lens Liveness and Dual-lens Livenes. By default, when one of the switches is turned on, the other one would be turned on simultaneously.<br>When the option is turned on or off, the device reboots automatically to execute the function. | |
| **Image Exposure Settings** | **Face AE:** When the face is in front of the camera in Face AE mode, the brightness of the face area increases, while other areas become darker.<br>**WDR:** Wide Dynamic Range (WDR) balances light and extends image visibility for surveillance videos under high contrast lighting scenes and | |

| | |
|---|---|
| | improves object identification under bright and dark environments.<br>**Anti-flicker Mode:** It is used when WDR is turned off. It helps to reduce flicker when the device's screen flashes at the same frequency as the light. |

***Note:***

1. Improper adjustment of the exposure and quality parameters may severely affect the performance of the device. Please adjust the exposure parameter only under the guidance of the after-sales service personnel of our company.
2. Face AE and Multi-face identifying are mutually exclusive options. When the Multi-face identifying feature switch is turned on, the Face AE switch will be automatically turned off. If you turn on Face AE at this time, the recognition mode will change to single face recognition mode.
3. The Face comparison interval and Tracking identification are mutually exclusive options. If the Tracking identification switch is turned on, the Face comparison interval function in the Face Identifying Settings will be disabled, and vice versa.

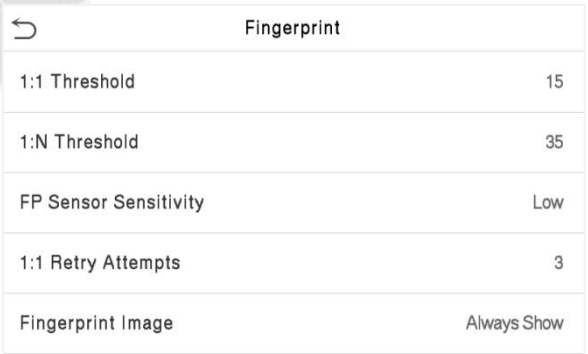
**Process to modify the Facial Recognition Accuracy**

- On the **System** interface, tap on **Face** > **Liveness Settings** and then toggle to enable Single-lens Liveness and Dual-lens Liveness to set the liveness settings.
- Then, on the main menu, tap **Autotest** > **Test Face** and perform the face test.
- Tap three times for the scores on the right upper corner of the screen, and the red rectangular box appears to start adjusting the mode.

  Keep one arm distance between the device and the face. It is recommended not to move the face in a wide range.

## 8.4 Fingerprint

Tap **Fingerprint** on the **System** interface to go to the Fingerprint parameter settings.



| Menu | Description |
|---|---|
| **1:1 Threshold** | Under 1:1 verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint template associated with the entered user ID enrolled in the device is greater than the set value. |
| **1:N Threshold** | Under 1:N verification method, the verification will only be successful when the similarity between the acquired fingerprint data and the fingerprint templates enrolled in the device is greater than the set value. |
| **FP Sensor Sensitivity** | To set the sensibility of fingerprint acquisition. It is recommended to use the default level "Medium". When the environment is dry, resulting in slow fingerprint detection, you can set the level to "High" to raise the sensibility; when the environment is humid, making it hard to identify the fingerprint, you can set the level to "Low". |
| **1:1 Retry Attempts** | In 1:1 Verification, users might forget the registered fingerprint, or press the finger improperly. To reduce the process of re-entering user ID, retry is allowed. |
| **Fingerprint Image** | To set whether to display the fingerprint image on the screen during fingerprint enrollment or verification. Four choices are available:<br>**Show for Enroll:** to display the fingerprint image on the screen only during enrollment.<br>**Show for Match:** to display the fingerprint image on the screen only during verification.<br>**Always Show:** to display the fingerprint image on screen during enrollment and verification.<br>**None:** Not to display the fingerprint image. |

## 8.5 Security Settings

Tap **Security Settings** on the **System** interface.

| Menu | Description |
|---|---|
| **Standalone Communication** | By default, this function is disabled. This function can be enabled or disabled via the menu interface. When it is switched on, a security prompt appears, and the device will restart after you confirm. |
| **SSH** | The device does not support the Telnet feature, hence SSH is typically used for remote debugging. By default, SSH is enabled. The menu interface allows you to enable and disable SSH. When enabled, there will be a security prompt, but the device will not need to be restarted after confirmation. |
| **User ID Masking** | After enabled, the User ID will be partially displayed after the personnel verification result (only the User ID with more than 2 digits supports the masking display), and it is enabled by default. |
| **Display Verification Name** | After enabled, the user's name will be displayed after the personnel verification result. The verification result will not show the name after disabling it. |
| **Save Photo as Template** | After disable this function, face re-registration is required after an algorithm upgrade. |

## 8.6 USB Upgrade

The device's firmware program can be upgraded with the upgrade file in a USB drive. Before conducting this operation, please ensure that the USB drive contains the correct upgrade file and is properly inserted into the device.

If no USB disk is inserted in, the system gives the following prompt after you tap USB Upgrade on the System interface.

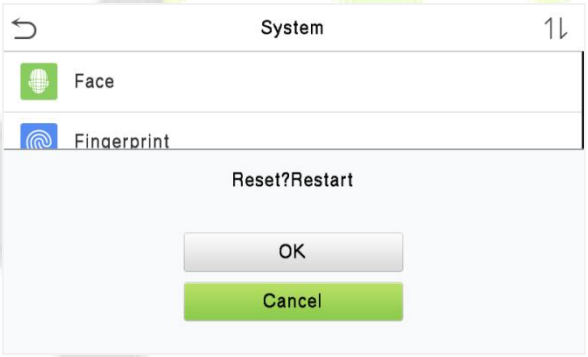
Tap **USB Upgrade** on the **System** interface.


***Note:*** If upgrade file is needed, please contact our technical support. Firmware upgrade is not recommenced under normal circumstances.

## 8.7 Factory Reset

This option restores the device, such as communication settings and system settings, to factory settings (does not clear registered user data).

Tap **Reset** on the **System** interface.

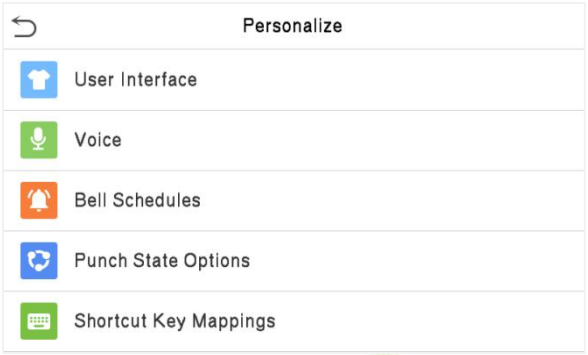



Tap **OK** to reset.

# 9 Personalize Settings

You may customize the interface settings, audio, and bell.

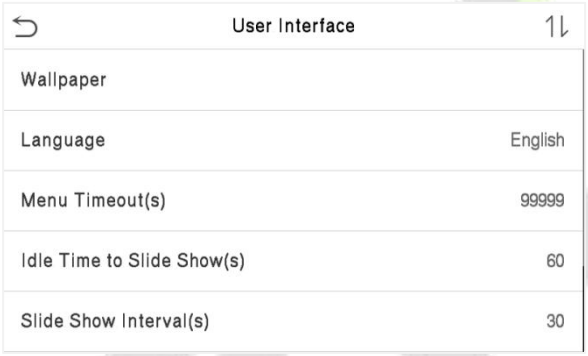
Tap **Personalize** on the main menu interface.

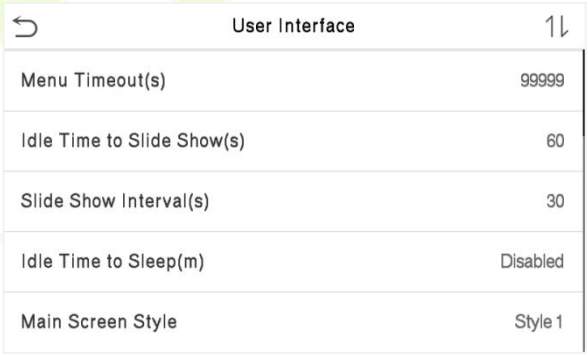



## 9.1 Interface Settings

You can customize the display style of the main interface.

Tap **User Interface** on the Personalize interface.



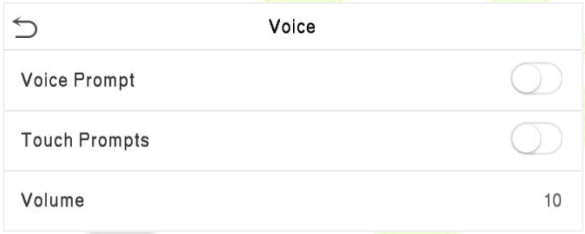




| Menu | Description |
|---|---|
| **Wallpaper** | To select the main screen wallpaper according to your personal preference. |
| **Language** | To select the language of the device. |
| **Menu Timeout (s)** | When there is no operation, and the time exceeds the set value, the device will automatically go back to the initial interface. You can disable the function or set the value between 60 and 99999 seconds. |
| **Idle Time to Slide Show (s)** | When there is no operation, and the time exceeds the set value, a slide show will be played. It can be disabled, or you may set the value between 3 |

| | |
|---|---|
| | and 999 seconds. |
| **Slide Show Interval (s)** | This refers to the time interval switching different slide show pictures. The function can be disabled, or you may set the interval between 3 and 999 seconds. |
| **Idle Time To Sleep (m)** | If you have activated the sleep mode, when there is no operation, the device will enter the standby mode. You can disable this function or set a value within 1-999 minutes. |
| **Main Screen Style** | To select the main screen style according to your personal preference. |

## 9.2 Voice Settings

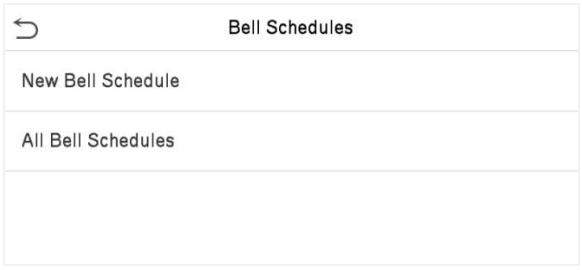
Tap **Voice** on the Personalize interface.




| Menu | Description |
|---|---|
| **Voice Prompt** | Select whether to enable voice prompts during operation. |
| **Touch Prompts** | Select whether to enable keypad sounds. |
| **Volume** | Adjust the volume of the device; valid value: 0 to 100. |

## 9.3 Bell Schedules

Tap **Bell Schedules** on the Personalize interface.



### Add a Bell

Tap **New Bell Schedule** to enter the adding interface:


| Menu | Description |
|---|---|
| **Bell Status** | Set whether to enable the bell status. |
| **Bell Time** | At this time of day, the device automatically rings the bell. |
| **Repeat** | Set the repetition cycle of the bell. |
| **Ring Tone** | Select a ring tone. |
| **Internal Bell Delay (s)** | Set the duration of the internal bell. Valid values range from 1 to 999 seconds. |

Back to the Bell Schedules interface; tap **All Bell Schedules** to view the newly added bell.

### Edit a Bell

On the All Bell Schedules interface, tap the bell to be edited.

Tap **Edit**, the editing method is the same as the operations of adding a bell.

### Delete a Bell

On the All Bell Schedules interface, tap the bell to be deleted.

Tap **Delete** and select [**Yes**] to delete the bell.

## 9.4 Punch States Options

Tap **Punch States Options** on the **Personalize** interface to configure the punch state settings.



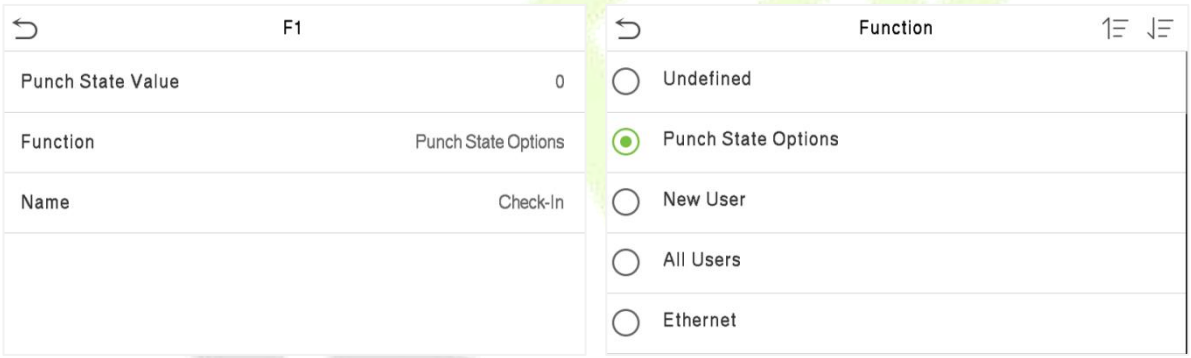
| Menu | Description |
|---|---|
| **Punch State Mode** | **Off:** Disable the punch state function. Therefore, the punch state key set under Shortcut Key Mappings menu will become invalid.<br><br>**Manual Mode:** Switch the punch state key manually, and the punch state key will disappear after Punch State Timeout.<br><br>**Auto Mode:** The punch state key will automatically switch to a specific punch status according to the predefined time schedule which can be set in the Shortcut Key Mappings.<br><br>**Manual and Auto Mode:** The main interface will display the auto-switch punch state key. However, the users will still be able to select alternative that is the manual attendance status. After timeout, the manual switching punch state key will become auto-switch punch state key.<br><br>**Manual Fixed Mode:** After the punch state key is set manually to a particular punch status, the function will remain unchanged until it is being manually switched again.<br><br>**Fixed Mode:** Only the manually fixed punch state key will be shown. Users cannot change the status by tapping any other keys. |

## 9.5 Shortcut Key Mappings

Users may define shortcut keys for attendance status and for functional keys which will be defined on the main interface. So, on the main interface, when the shortcut keys are taped, the corresponding attendance status or the function interface will be displayed directly.

Tap **Shortcut Key Mappings** on the **Personalize** interface to set the required shortcut keys.


- On the **Shortcut Key Mappings** interface, tap on the required shortcut key to configure the shortcut key settings.
- On the **Shortcut Key** (that is "F1") interface, tap **function** to set the functional process of the shortcut key either as punch state key or function key.
- If the Shortcut key is defined as a function key (such as New user, All users, etc.), the configuration is completed as shown in the image below.



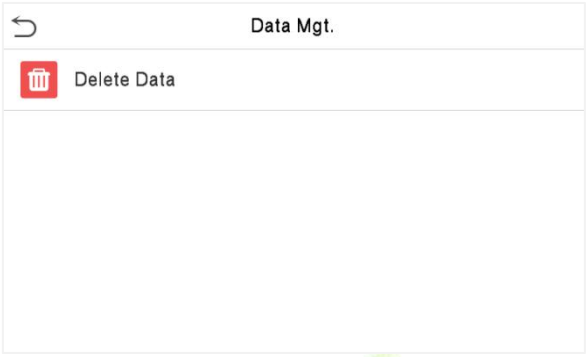

- If the Shortcut key is set as a punch state key (such as check in, check out, etc.), then it is required to set the punch state value (valid value 0~250), name.

***Note:*** When the function is set to Undefined, the device will not enable the punch state key.

# 10 Data Management

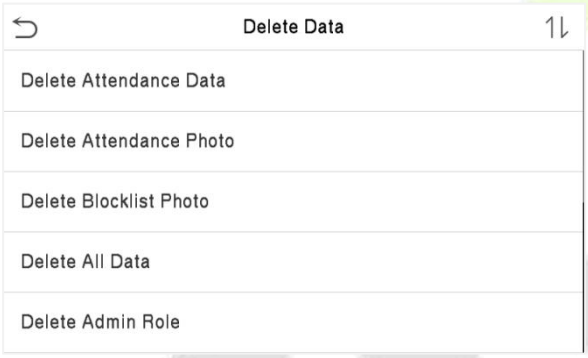
The Data Management is used to delete the relevant data in the device.

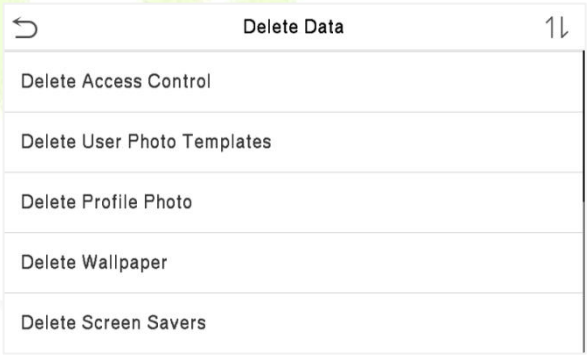
Tap **Data Mgt.** on the main menu interface.




## 10.1 Delete Data

Tap **Delete Data** on the Data Mgt. interface.



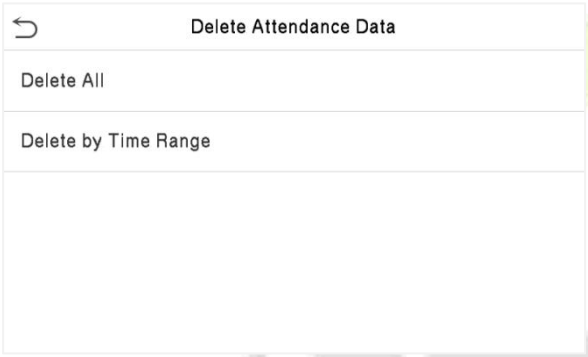




| Menu | Description |
|---|---|
| **Delete Attendance Data** | To delete attendance data conditionally. |
| **Delete Attendance Photo** | To delete attendance photos of designated personnel. |
| **Delete Blocklist Photo** | To delete the photos taken during failed verifications. |
| **Delete All Data** | To delete information and attendance logs/access records of all registered users. |
| **Delete Admin Role** | To remove all administrator privileges. |
| **Delete Access Control** | To delete all access data. |

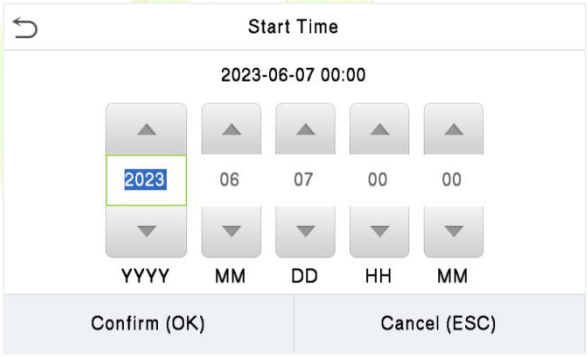
| | |
|---|---|
| **Delete User Photo Templates** | To delete user photo templates in the device. When deleting template photos, there is a risk reminder: "Face re-registration is required after an algorithm upgrade." |
| **Delete Profile Photo** | To delete all the profile photos on the device. |
| **Delete Wallpaper** | To delete all wallpapers in the device. |
| **Delete Screen Savers** | To delete the screen savers in the device. |

The user may select Delete All or Delete by Time Range when deleting the access records, attendance photos or block listed photos. Selecting Delete by Time Range, you need to set a specific time range to delete all data within a specific period.

Select Delete by Time Range



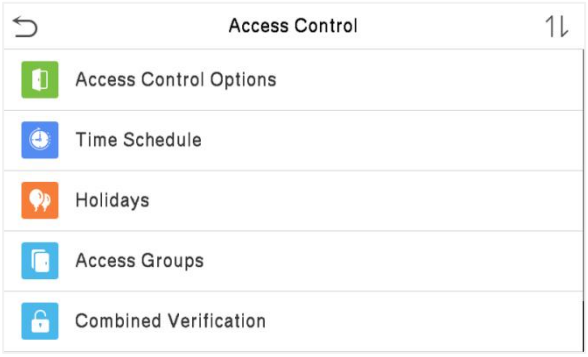

Set the time range and tap OK

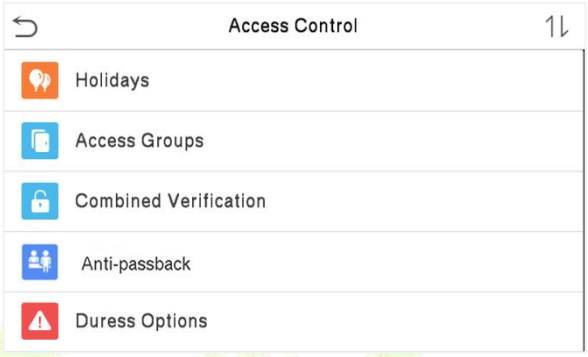


# 11 Access Control

Access Control is used to set the schedule of a door opening, locks control and other parameter settings related to access control.

Tap **Access Control** on the main menu interface.




**To gain access, the registered user must meet the following conditions:**

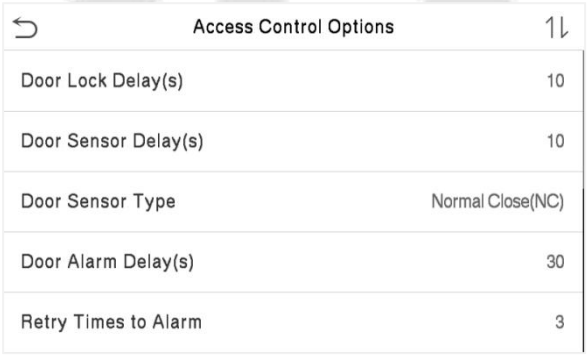
1. The current door unlock time should be within any valid time zone of the user time period.
2. The user's group must be in the door unlock combination (when there are other groups in the same access combo, verification of members of those groups are also required to unlock the door).

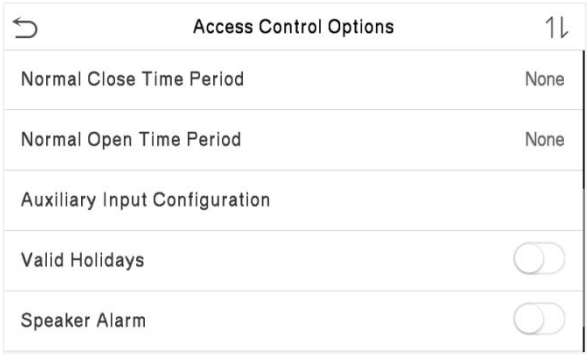
In default settings, new users are allocated into the first group with the default group time zone and access combo as "1" and set in an unlocking state.

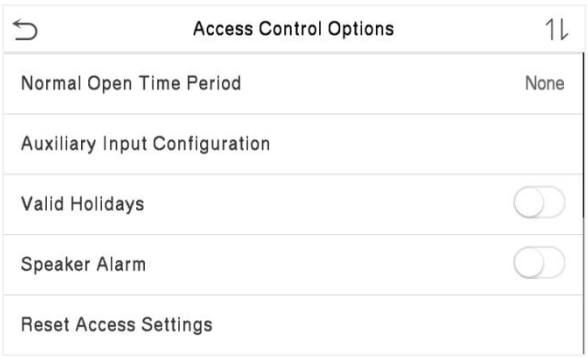
## 11.1 Access Control Options

This option is used to set the parameters of the control lock of the device and the related parameters.

Tap **Access Control Options** on the Access Control interface.






| Menu | Description |
|---|---|
| **Door Lock Delay (s)** | The length of time that the device controls the electric lock to be in unlock state.<br>Valid value: 1 to 10 seconds; 0 seconds represents disabling the function. |
| **Door Sensor Delay (s)** | If the door is not locked and is left open for a certain duration (Door Sensor Delay), an alarm will be triggered.<br>The valid value of Door Sensor Delay ranges from 1 to 255 seconds. |
| **Door Sensor Type** | There are three Sensor types: None, Normal Open, and Normal Closed.<br>**Normally Open(NO):** It means the door is always left open when electric power is on.<br>**Normally Closed(NC):** It means the door is always left closed when electric power is on.<br>**None:** It means the door sensor is not in use. |
| **Door Alarm Delay (s)** | When the state of the door sensor is inconsistent with that of the door sensor type, an alarm will be triggered after a specified time period, i.e. the Door Alarm Delay. The valid value ranges from 1 to 999 seconds. 0 means immediate alarm. |
| **Retry Time to Alarm** | When the number of failed verification reaches a set value, which ranges from 1 to 9 times, an alarm will be triggered. If the set value is "None", the alarm will never be triggered due to failed verifications. |
| **Normal Close Time Period** | Scheduled time period for "Normal Close" mode, so that no one can gain access during this period. |

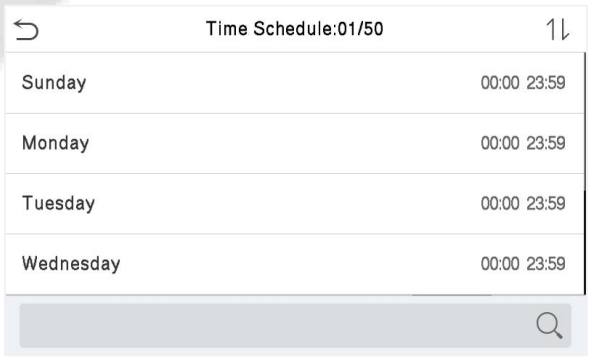
| | |
|---|---|
| **Normal Open Time Period** | It is the scheduled time-period for "Normal Open" mode so that the door is always open during this period. |
| **Auxiliary Input Configuration** | Sets the door unlock time period and auxiliary output type of the auxiliary terminal device. Auxiliary output types include None, Trigger door open, Trigger Alarm, Trigger door open and Alarm. |
| **Valid Holiday** | To set if Normal Close Period or Normal Open Period settings are valid in set holiday time period. Choose ON to enable the functions during holiday. |
| **Speaker Alarm** | It transmits a sound alarm or disassembly alarm from the local. When the door is closed or the verification is successful, the system cancels the alarm from the local. |
| **Reset Access Setting** | The access control reset parameters include door lock delay, door sensor delay, door sensor type, verification mode, door available time period, normal open time period, master device, and alarm. However, erased access control data in Data Mgt. is excluded. |

## 11.2 Time Schedule

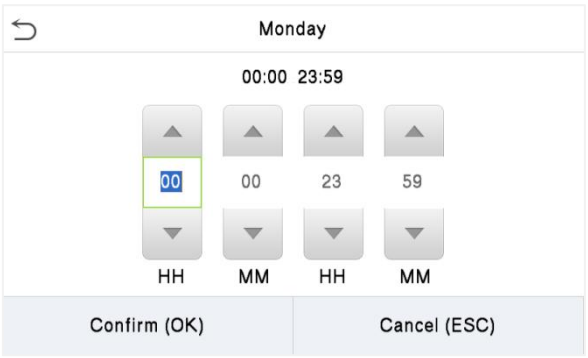
Tap **Time Schedule** on the Access Control interface to configure the time settings.

- The entire system can define up to 50 Time Periods.
- Each time-period represents **7** Time Zones, i.e., **1** week, and each time zone is a standard 24 hour period per day and the user can only verify within the valid time-period.
- The Time Zone format of each time-period is **HH MM-HH MM**, which is accurate to minutes according to the 24-hour clock.

Tap the grey box to search the required Time Zone and specify the required Time Zone number (maximum up to 50 zones).




Click the date on which time zone settings is required. Enter the starting and ending time, and then tap OK.




***Note:***

1. The door is inaccessible for the whole day when the End Time occurs before the Start Time (such as 23:57~23:56).
2. It is the time interval for valid access when the End Time occurs after the Start Time (such as 08:00~23:59).
3. The door is accessible for the whole day when the End Time occurs after the Start Time (such that Start Time is 00:00 and End Time is 23:59).
4. The default Time Zone 1 indicates that the door is open all day long.

## 11.3 Holiday Settings

Whenever there is a holiday, you may need a special access time; but changing everyone's access time one by one is extremely cumbersome, so you can set a holiday access time which applies to all the employees, and the user will be able to open the door during the holidays.

Tap **Holidays** on the Access Control interface.


### Add a New Holiday

Tap **Add Holiday** on the Holidays interface and set the holiday parameters.


### Edit a Holiday

On the Holidays interface, select a holiday item to be modified. Tap **Edit** to modify holiday parameters.

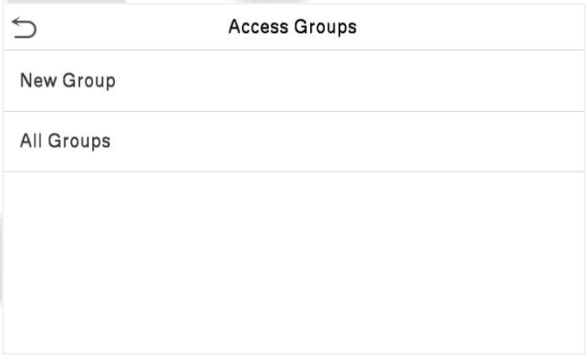
### Delete a Holiday

On the Holidays interface, select a holiday item to be deleted and tap **Delete**. Tap **OK** to confirm the deletion. After deletion, this holiday is no longer displayed on All Holidays interface.

## 11.4 Access Groups

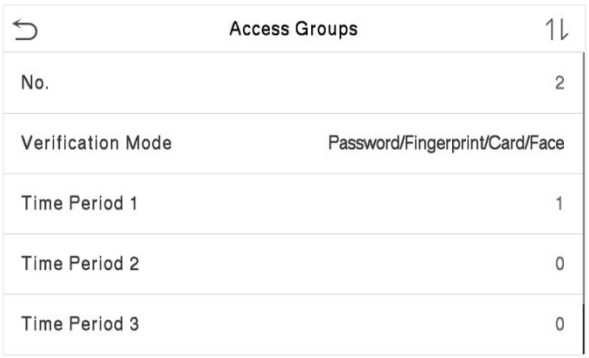
This is to easily manage groupings and users in different access groups. Settings of an access group such as access time zones are applicable to all members in the group by default. However, users may manually set the time zones as needed. User authentication takes precedence over group authentication when group authentication modes overlap with the individual authentication methods. Each group can set a maximum of three time zones. By default, newly enrolled users are assigned to Access Group 1; they can be assigned to other access groups.

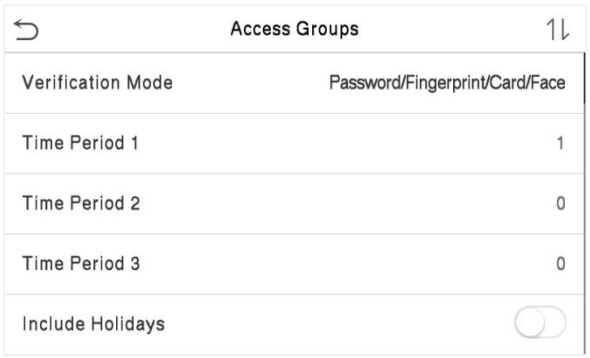
Click **Access Groups** on the Access Control interface.




### Add a New Group

Click **New Group** on the Access Groups interface and set access group parameters.




***Note:***

1. There is a default access group numbered 1, which cannot be deleted, but can be modified.
2. A number cannot be modified after being set.
3. When the holiday is set to be valid, personnel in a group may only open the door when the group time zone overlaps with the holiday time period.
4. When the holiday is set to be invalid, the access control time of the personnel in a group is not affected during holidays.

### Edit a Group

On the All Groups interface, select the access group item to be modified. Click Edit and modify access group parameters.

### Delete a Group

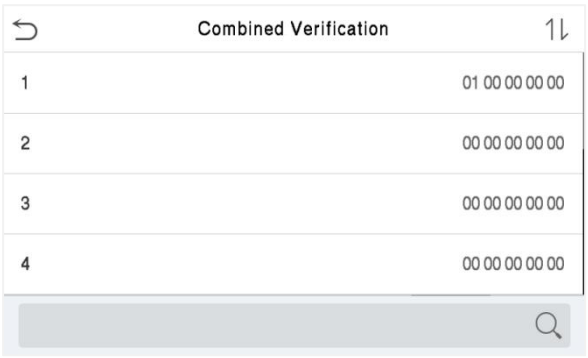
On the All Groups interface, select the access group item to be deleted and click Delete. Click OK to confirm deletion. The deleted access group is no longer displayed in All Groups.

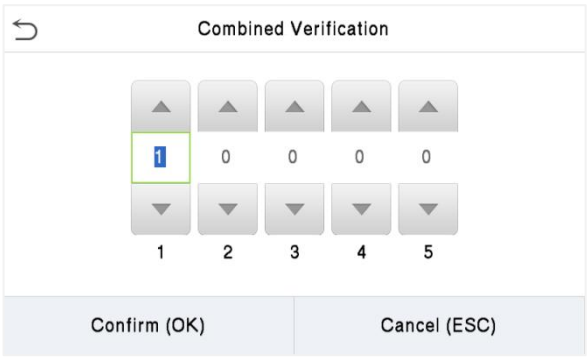
## 11.5 Combined Verification Settings

Access groups are arranged into different door-unlocking combinations to achieve multiple verifications and strengthen the security.

In a door-unlocking combination, the range of the combined number N is: $0 \leq N \leq 5$, and the number of members N may all belong to one access group or may belong to five different access groups.

Click **Combined Verification** on the Access Control interface.




Tap the door-unlocking combination to be set. Tap the up and down arrows to input the combination number, then tap OK.

**Examples:**

- The **Door-unlocking combination** 1 is set as (**01 03 05 06 08**), indicating that the unlocking combination 1 consists of 5 people, and the 5 individuals are from 5 groups, namely, **Access Control Group 1** (AC group 1), AC group 3, AC group 5, AC group 6, and AC group 8, respectively.
- The **Door-unlocking combination 2** is set as (**02 02 04 04 07**), indicating that the unlocking combination 2 consists of 5 people; the first two are from AC group 2, the next two are from AC group 4, and the last person is from AC group 7.
- The **Door-unlocking combination 3** is set as (**09 09 09 09 09**), indicating that there are 5 people in this combination; all of which are from AC group 9.
- The **Door-unlocking combination 4** is set as (**03 05 08 00 00**), indicating that the unlocking combination 4 consists of three people. The first person is from AC group 3, the second person is from AC group 5, and the third person is from AC group 8.

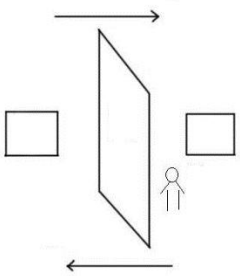
**Delete a Door-unlocking Combination**

Set all the group numbers as 0 if you want to delete door-unlocking combinations.

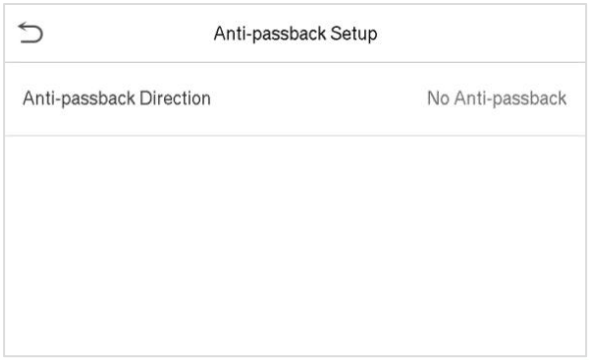
## 11.6 Anti-passback Setup

It is possible that users may be followed by some persons to enter the door without verification, resulting in a security breach. So, to avoid such a situation, the Anti-Passback option was developed. Once it is enabled, the check-in record must match with the check-out record so as to open the door.

This function requires two devices to work together: one is installed inside the door (master device), and the other one is installed outside the door (slave device). The two devices communicate via the Wiegand signal. The Wiegand format and Output type (User ID / Card Number) adopted by the master device and slave device must be consistent.



Tap **Anti-passback Setup** on the Access Control interface.



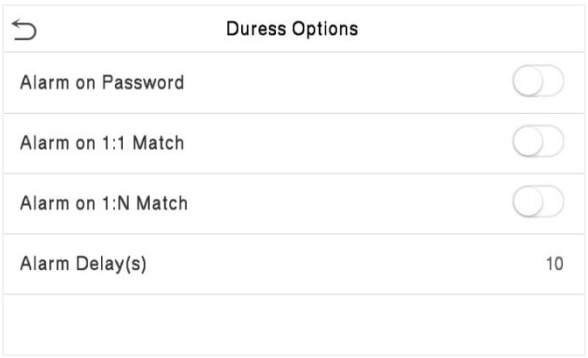


| Menu | Description |
|---|---|
| **Anti-passback direction** | **No Anti-passback:** Anti-passback function is disabled, which means successful verification through either the master device or slave device can unlock the door. The attendance state is not saved in this option.<br>**Out Anti-passback:** After a user checks out, only if the last record is a check-in record, the user can check-out again; otherwise, the alarm will be triggered. However, the user can check-in freely.<br>**In Anti-passback:** After a user checks in, only if the last record is a check-out record, the user can check-in again; otherwise, the alarm will be triggered. However, the user can check-out freely.<br>**In/Out Anti-passback:** After a user checks in/out, only if the last record is a check-out record, the user can check-in again; or if it is a check-in record, the user can check-out again; otherwise, the alarm will be triggered. |

## 11.7 Duress Options Settings

If a user activated the duress verification function with specific authentication method(s), when he/she is under coercion during authentication with such method, the device will unlock the door as usual, but at the same time a signal will be sent to trigger the alarm.

Tap **Duress Options** on the Access Control interface.



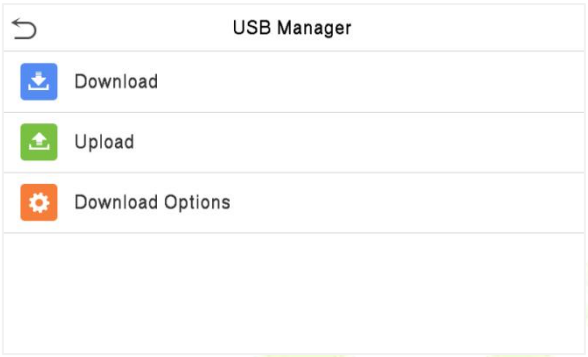

| Menu | Description |
|---|---|
| **Alarm on Password** | When a user uses the password verification method, an alarm signal will be generated, otherwise there will be no alarm signal. |
| **Alarm on 1:1 Match** | When a user uses any fingerprint to perform the 1:1 verification, an alarm signal will be generated, otherwise there will be no alarm signal. |
| **Alarm on 1:N Match** | When a user uses any fingerprint to perform 1:N verification, an alarm signal will be generated, otherwise there will be no alarm signal. |
| **Alarm Delay (s)** | Alarm signal will not be transmitted until the alarm delay time is elapsed. The value ranges from 1 to 999 seconds. |

# 12 USB Manager

You can import the user information, and attendance data in the machine to matching attendance software for processing by using a USB disk, or import the user information to other devices for backup.

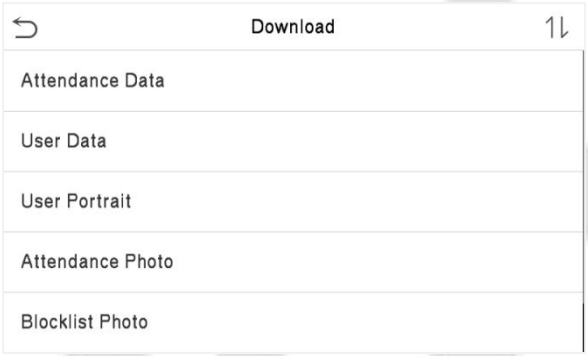
Before uploading/downloading data from/to the USB disk, insert the USB disk into the USB slot first.

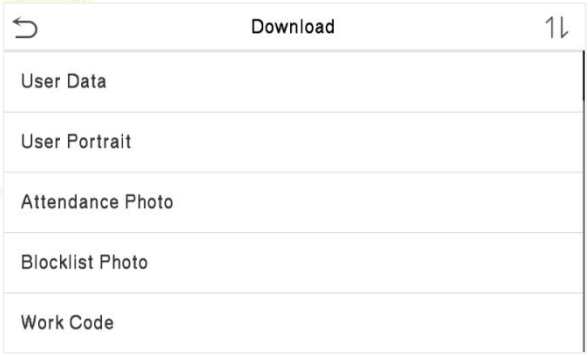
Tap **USB Manager** on the main menu interface.




## 12.1 USB Download

On the **USB Manager** interface, tap **Download**.



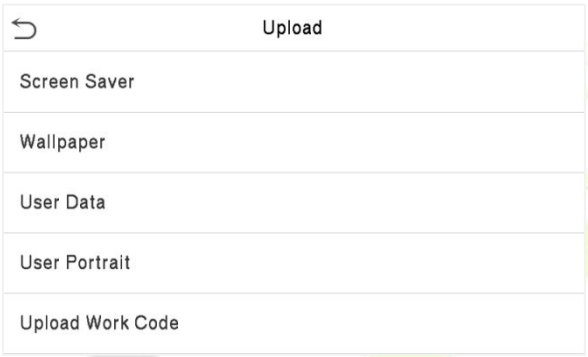

| Menu | Description |
|---|---|
| **Attendance Data** | To download attendance record in specified time period into USB disk. |
| **User Data** | To download all user information from the device into USB disk. |
| **User Portrait** | To download all user portraits from the device into a USB disk. |
| **Attendance Photo** | To download all attendance photos from the device into USB disk. |
| **Blocklist Photo** | To download all blocklisted photos (photos taken after failed verifications) |

| | |
|---|---|
| | from the device into USB disk. |
| **Work Code** | To download all work code from the device into USB disk. |

***Note:*** If the user's capacity exceeds 30000, be sure to use **exFAT format** when downloading data using USB disk.

## 12.2 USB Upload

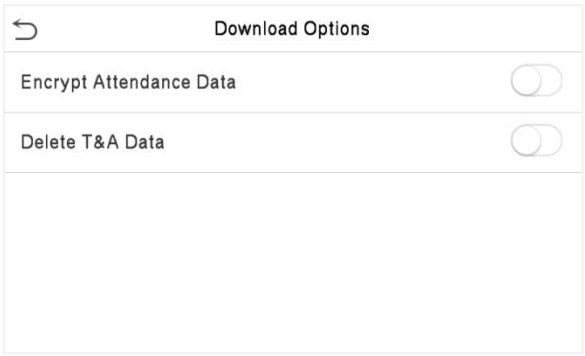
On the **USB Manager** interface, tap **Download**.




| Menu | Description |
|---|---|
| **Screen Save** | To upload all screen savers from USB disk into the device. You can choose Upload selected photo or Upload all photos. The images will be displayed on the device's main interface after upload. |
| **Wallpaper** | To upload all wallpapers from USB disk into the device. You can choose Upload selected photo or Upload all photos. The images will be displayed on the screen after upload. |
| **User Data** | To upload all the user information from USB disk into the device. |
| **User Portrait** | To upload all user portraits from USB disk into the device. |
| **Upload Work Code** | To upload all work code from USB disk into the device. |

## 12.3 Download Options

On the **USB Manager** interface, tap **Download Options**.

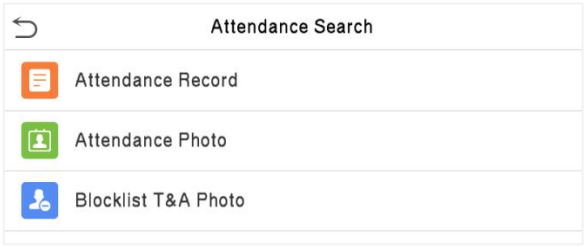



| Menu | Description |
|---|---|
| **Encrypt Attendance Date** | The attendance data is encrypted during the uploading and downloading. |
| **Delete T&A Data** | After successful downloading, the attendance data on the device is deleted. |

# 13 Attendance Search

Once the identity of a user is verified, the access record is saved in the device. This function enables users to check their event logs.

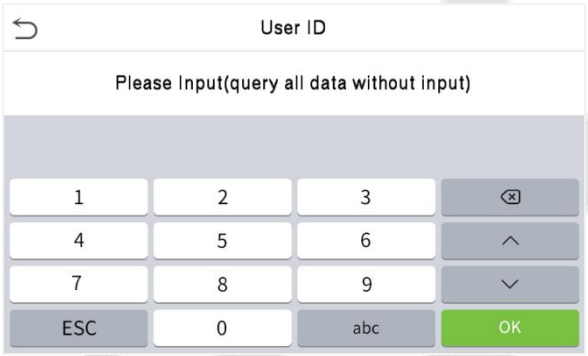
Select **Attendance Search** on the main menu interface to search for the required record.




The process of searching for attendance and blocklist photos is similar to that of searching for attendance record. The following is an example of searching for attendance record.

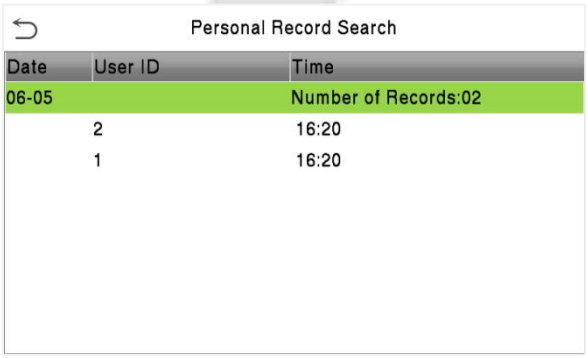
On the **Attendance Search** interface, tap **Attendance Record** to search for the required record.

1. Enter the user ID to be searched and tap OK. If you want to search for records of all users, tap OK without entering any user ID.




2. Select the time range in which the records you want to search for.


3. The record search succeeds. Tap the record in green to view its details.

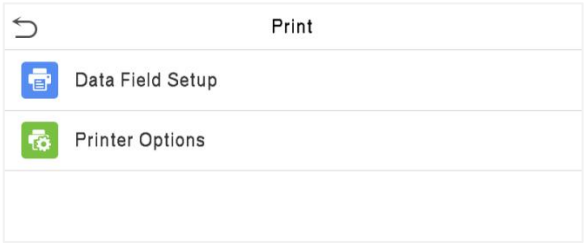



4. The below figure shows the details of the selected record.

# 14 Print Settings

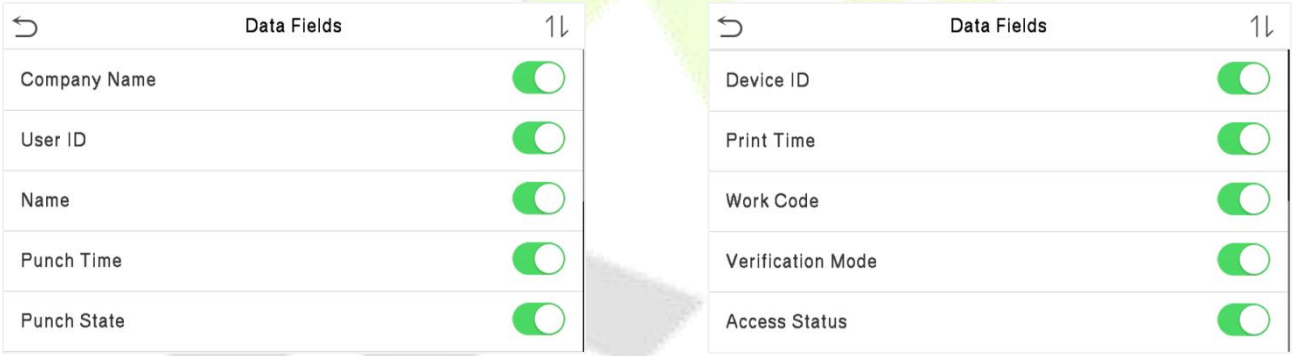
Devices with the printing function can print attendance records when a printer is connected (this function is optional and only implemented in some products).

Tap **Print** on the Main Menu interface.




## 14.1 Print Data Field Settings

Select **Data Field Setup** on the P**rint in**terface. Toggle button to turn on/off the fields requiring a print.




## 14.2 Print Options Settings

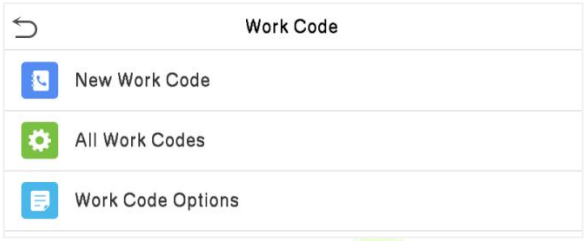
Select the **Printer Options** on the **Print** interface. Toggle button to enable or disable the **Paper Cut** function.


***Note:*** To turn on the **Paper Cut** function, it is required to connect the device with a printer with paper cutting function, so that the printer will cut papers according to the selected printing information while printing.

# 15 Work Code

Employees' salaries are subject to their attendance records. An employee can be engaged in more than one type of work which may vary with time. As the pay varies according to the work types, the FFR terminal provides a parameter to indicate the corresponding work type for every attendance record to facilitate rapid understanding of different attendance situations during the handling of attendance data.

Tap **Work Code** on the main menu interface.




## 15.1 Add a Work Code

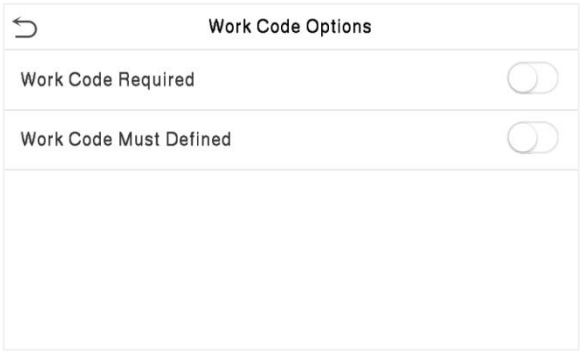

| Menu | Description |
|---|---|
| **ID** | It is the digital code of the work code. Users may set a valid value between 1 and 99999999. |
| **Name** | It is the naming of the work code. |

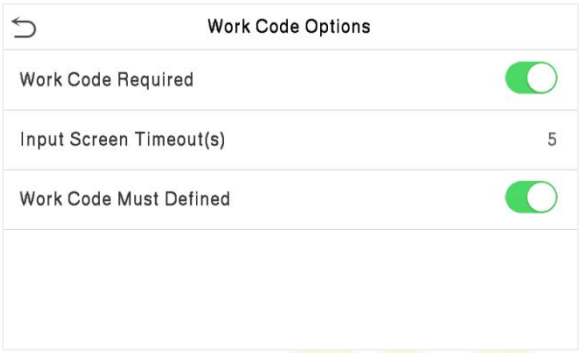
## 15.2 All Work Codes

You can view, edit and delete work codes in All Work Codes. The process of editing a work code is the same as adding a work code, except that the ID is not allowed to be modified.

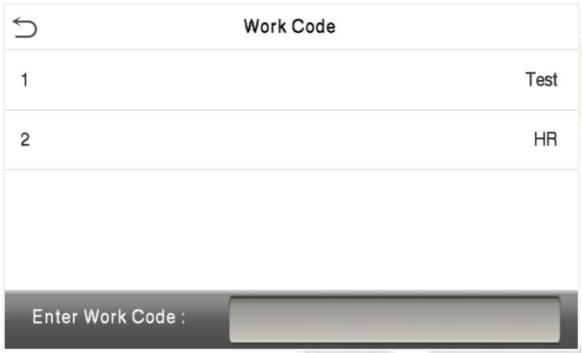
## 15.3 Work Code Options

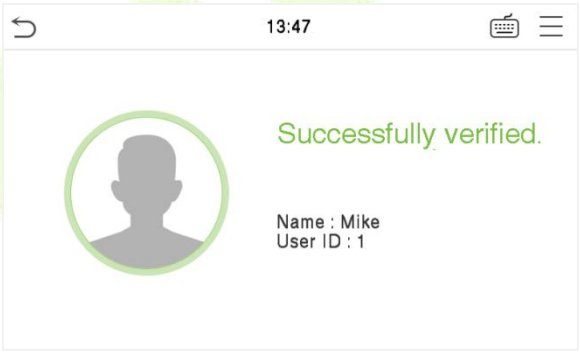
To set whether entering the work code is a must and whether the entered work code must exist during authentication.




In **1: N** or **1:1** verification, the system will automatically pop up the following window. Select the corresponding Word Code manually to verify successfully.

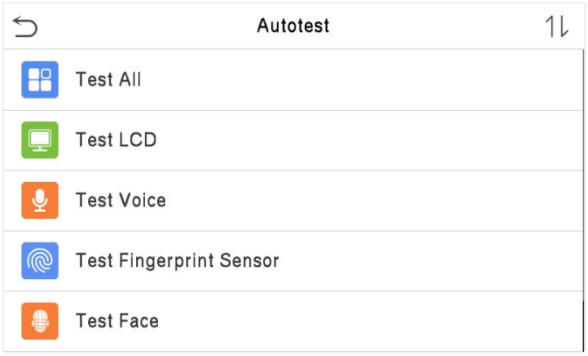


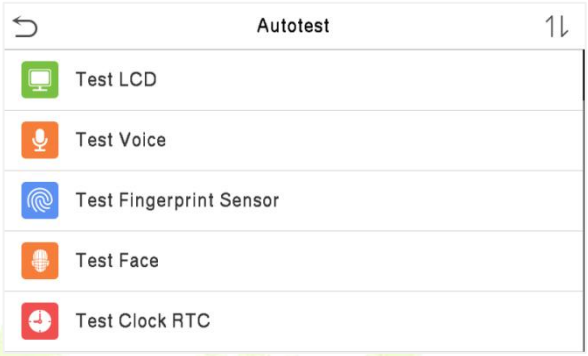



# 16 Autotest

To automatically test whether all modules in the device function properly, which include the LCD, Audio, Camera, fingerprint and real-time clock (RTC).

Tap **Autotest** on the main menu interface.



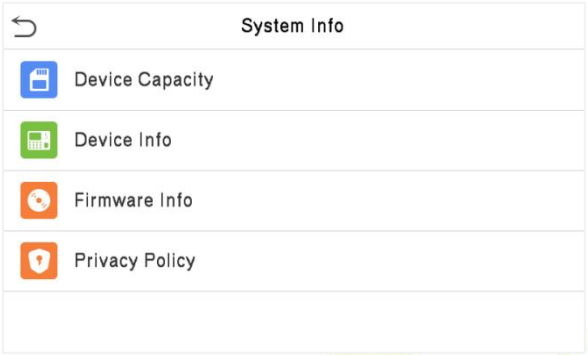




| Menu | Description |
|---|---|
| **Test All** | To automatically test whether the LCD, audio, camera, fingerprint and RTC are normal. |
| **Test LCD** | To automatically test the display effect of LCD screen by displaying full-color, pure white, and pure black to check whether the screen displays the colors normally. |
| **Test Voice** | To automatically test whether the audio files stored in the device are complete and the voice quality is good. |
| **Test Fingerprint Sensor** | To test the fingerprint sensor by pressing a finger on the scanner to check if the acquired fingerprint image is clear. When you are pressing a finger on the scanner, the fingerprint image will display on the screen. |
| **Test Face** | To test if the camera functions properly by checking the pictures taken to see if they are clear enough. |
| **Test Clock RTC** | To test the RTC. The device tests whether the clock works normally and accurately with a stopwatch. Touch the screen to start counting and tap it again to stop counting. |

# 17 System Information

With the system information option, you can view the storage status, the version information of the device, and so on.

Click **System** Info on the main menu interface.




| Menu | Description |
|---|---|
| **Device Capacity** | Displays the current device's user storage, password, fingerprint, face and card ★ storage, administrators, attendance records, attendance and blocklist photos. |
| **Device Info** | Displays the Device's name, Serial number, MAC Address, Face and fingerprint algorithm version information, platform information, MCU Version, manufacturer and manufacture Date. |
| **Firmware Info** | Displays the Firmware version and other version information of the device. |
| **Privacy Policy** | The privacy policy control will appear when the gadget turns on for the first time. After tapping "**I have read it**," the customer can use the product regularly. Tap **System Info** -> **Privacy Policy** to view the content of the privacy policy. The privacy policy's content does not allow for U disc export.<br><br>**Note:** The current privacy policy's text is only available in Simplified Chinese/English. However, translation of other multi-language content is underway, with more iterations. |

# Appendix 1

## Requirements of Live Collection and Registration of Visible Light Face Templates

1) It is recommended to perform registration in an indoor environment with an appropriate light source without underexposure or overexposure.
2) Do not shoot towards outdoor light sources like door or window or other strong light sources.
3) Dark-color apparels which are different from the background color are recommended for registration.
4) Please show your face and forehead, and do not cover your face and eyebrows with your hair.
5) It is recommended to show a plain facial expression. Smile is acceptable, but do not close your eyes, or incline your head to any orientation. Two images are required for persons with eyeglasses, one image with eyeglasses and one other without.
6) Do not wear accessories like scarf or mask that may cover your mouth or chin.
7) Please face right towards the capturing device, and locate your face in the image capturing area as shown in Image 1.
8) Do not include more than one face in the capturing area.
9) 50cm - 80cm is recommended for capturing distance adjustable subject to body height.


Image1 Face Capture Area

# Requirements for Visible Light Digital Face Template Data

Digital photo should be straightly edged, colored, half-portrayed with only one person, and the person should be uncharted and not in uniform. Persons who wear eyeglasses should remain to put on eyeglasses for photo capturing.

- **Eye Distance**

200 pixels or above are recommended with no less than 115 pixels of distance.

- **Facial Expression**

Plain face or smile with eyes naturally open are recommended.

- **Gesture and Angel**

Horizontal rotating angle should not exceed ±10°, elevation should not exceed ±10°, and depression angle should not exceed ±10°.

- **Accessories**

Masks and colored eyeglasses are not allowed. The frame of the eyeglasses should not shield eyes and should not reflect light. For persons with thick eyeglasses frame, it is recommended to capture two images, one with eyeglasses and the other one without.

- **Face**

Complete face with clear contour, real scale, evenly distributed light, and no shadow.

- **Image Format**

Should be in BMP, JPG or JPEG.

- **Data Requirement**

Should comply with the following requirements:

1) White background with dark-colored apparel.
2) 24bit true color mode.
3) JPG format compressed image with not more than 20kb size.
4) Definition rate between 358 x 441 to 1080 x 1920.
5) The vertical scale of head and body should be 2:1.
6) The photo should include the captured person's shoulders at the same horizontal level.
7) The captured person should be eyes-open and with clearly seen iris.
8) Plain face or smile is preferred, showing teeth is not preferred.
9) The captured person should be clearly seen, natural in color, and without image obvious twist, no shadow, light spot or reflection in face or background, and appropriate contrast and lightness level.

# Appendix 2

## Privacy Policy

**Notice:**

To help you better use the products and services of ZKTeco (hereinafter referred as "we", "our", or "us") a smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

**Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.**

### I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

### II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the**

**Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**

2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

## III. How We Handle Personal Information of Minors

Our products, website and services are mainly designed for adults. Without consent of parents or guardians, minors shall not create their own account. If you are a minor, it is recommended that you ask your parents or guardian to read this Policy carefully, and only use our services or information provided by us with consent of your parents or guardian.

We will only use or disclose personal information of minors collected with their parents' or guardians' consent if and to the extent that such use or disclosure is permitted by law or we have obtained their parents' or guardians' explicit consent, and such use or disclosure is for the purpose of protecting minors.

Upon noticing that we have collected personal information of minors without the prior consent from verifiable parents, we will delete such information as soon as possible.

## IV. Others

You can visit https://www.zkteco.com/en/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

# Eco-friendly Operation

The product's "eco-friendly operational period" refers to the time during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

**Hazardous or Toxic substances and their quantities**

| Component Name | Hazardous/Toxic Substance/Element | | | | | |
|---|---|---|---|---|---|---|
| | Lead (Pb) | Mercury (Hg) | Cadmium (Cd) | Hexavalent Chromium (Cr6+) | Polybrominated Biphenyls (PBB) | Polybrominated Diphenyl Ethers (PBDE) |
| Chip Resistor | × | ○ | ○ | ○ | ○ | ○ |
| Chip Capacitor | × | ○ | ○ | ○ | ○ | ○ |
| Chip Inductor | × | ○ | ○ | ○ | ○ | ○ |
| Diode | × | ○ | ○ | ○ | ○ | ○ |
| ESD component | × | ○ | ○ | ○ | ○ | ○ |
| Buzzer | × | ○ | ○ | ○ | ○ | ○ |
| Adapter | × | ○ | ○ | ○ | ○ | ○ |
| Screws | ○ | ○ | ○ | × | ○ | ○ |

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in SJ/T 11363—2006.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in SJ/T 11363—2006.

**Note**: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the

current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com